



جامعة العربي التبسي - تبسة - الجزائر

كلّية الحقوق والعلوم السياسية

قسم العلوم السياسية

مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في العلوم السياسية

تخصص: دراسات إستراتيجية و أمنية

بعنوان:

الإستراتيجية الروسية لمكافحة التهديدات الإلكترونية "الأمن السيبراني في عهد فلاديمير بوتين 2009 - 2014 "

إعداد الطالبين:

- بعلوج السعيد.
- رزقي جلال.

إشراف الأستاذ:

- د. البار أمين.

أعضاء لجنة المناقشة:

الاسم واللقب	الصفة	الرتبة العلمية
د/يوسف ازروال	رئيسا	أستاذ محاضر -أ-
د/البار أمين	مشرفا ومقررا	أستاذ محاضر -أ-
أ/بوحريص الصديق	ممتحنا	أستاذ مساعد -أ-

السنة الجامعية: 2018 – 2019



جامعة العربي التبسي - تبسة - الجزائر

كلّية الحقوق والعلوم السياسية

قسم العلوم السياسية



مذكرة مقدمة ضمن متطلبات نيل شهادة الماستر في العلوم السياسية

تخصص: دراسات إستراتيجية و أمنية

بعنوان:

الإستراتيجية الروسية لمكافحة التهديدات الإلكترونية "الأمن السيبراني في عهد فلاديمير بوتين 2009 - 2014 "

إعداد الطالبين:

- بعلوج السعيد.
- رزقي جلال.

إشراف الأستاذ:

- د. البار أمين.

أعضاء لجنة المناقشة:

الاسم واللقب	الصفة	الرتبة العلمية
د/يوسف ازروال	رئيسا	أستاذ محاضر -أ-
د/البار أمين	مشرفا ومقررا	أستاذ محاضر -أ-
أ/بوحريص الصديق	ممتحنا	أستاذ مساعد -أ-

السنــة الجامعيــة: 2018 – 2019



University Larbi Tebessi-Tebessa- Algeria
Faculty of Law and political sciences
Department of political science



An additional thesis to the requirements to obtaining of the Master Degree in Political sciences

Specialty: Strategic Studies

Russian strategy to confront cyber threats "Cyber Security" in the period of "Vladimir Putin" 2009 - 2014 "

By students :
- Said Baaloudj.
- Djalal Rezgui.

Under the Supervision of Prof :
Dr. ELBAR Amin

The member of Panel of deliberation

Nam and First Name	Scientific Statuts	Qality in the research
YOUCEF AZEROUAL	DOCTOR	President
Dr. ELBAR AMIN	DOCTOR	Supervison and rapporteur
BOUHRIS SEDIK	PROFESSOR	Discoursed

Academic Year : 2018/2019



﴿وَقُلِ اعْمَلُوا فَسَيَرَى اللَّهُ عَمَلَكُمْ وَرَسُولُهُ وَالْمُؤْمِنُونَ﴾

سورة التوبة الآية [105]

صدق الله العظيم

شكر وتقدير

الحمد لله وكفى، وصلى الله وبارك على نبيّه وعباده الذين اصطفى، صاحب العزّة والمنان، اللهم افتح لنا بابا نفد منه إليك، سبحانك لك مقاليد السماوات والأرض، وأنت على كلّ شيء قدير، يقول الله عزّ وجلّ في محكم تنزيله: {لَئِنْ شَكَرْتُمْ لَأَزِيدَنَّكُمْ} (سورة إبراهيم الآية 07).

إنّه من دواعي الغبطة والسرور أن وفقّنا الله تعالى إلى إتمام هذا العمل المتواضع، ذلك بفضل ترجّيه ونصائح المشرف الفاضل الدكتور "البار أمين" الذي لم يقصّر في إسداد النصح والإرشاد والتوجيه وتقديم الإستشارة مع الصبر والأناة والتي كانت تزيدنا ثقة وسيرا إلى بلوغ غاية المرام، وإخراج هذا العمل على أحسن وجه فجزاه الله عنّا خير الجزاء.

كما نتوجّه بخالص الشكر والإمتنان لأعضاء اللجنة المشرفة على تفضّلهم بقبول مناقشة هذا العمل.

ولا ننسى كافة أساتذة كلية العلوم السياسية بجامعة العربي التبسي – تبسة.

ملخص:

تتمحور هذه الدراسة حول دور الاستراتيجية الروسية في مواجهة التهديدات الالكترونية وذلك بهدف اعطاء رؤية شاملة للاستراتيجية الروسية ودورها في تحقيق امنها السيبراني ،حيث اضافت حملة جديدة ،تتمثل في اعادة صياغة قواعد الفضاء السيبراني العالمي والحد من تنامي التهديدات السيبرانية والدفاع الالكتروني .حيث يختلف المنظور الروسي للحرب السيبرانية بشكل واضح عن نظرائه الغربيين ،ويبدو ذلك واضحا من خلال الطريقة التي يعرف بها المنظرون الروس الحرب السيبرانية ،والتي تشير الى كيفية تحكم روسيا للفضاء السيبراني لتحقيق الاهداف القومية لروسيا الاتحادية .

حيث تختص روسيا في التعامل مع مختلف التحديات الامنية الالكترونية و المخاطر السيبرانية ،من خلال وضع خطط استراتيجية لمكافحة تلك التهديدات و تحقيق امن سيبراني وطني .

ممّا دفع روسيا الى فرض عقيدة جديدة تتمثل في وجود قيود على الخدمات التي تخص وسائل النفوذ الاعلامي التي تمارسها البلدان الاخرى بهدف زعزعة الاستقرار السياسي الداخلي والخارجي في روسيا.

Summary:

The study focuses on the Russian strategy in the face of cyber threats, in order to give a comprehensive account of the Russian strategy and its role in achieving its cyber security, adding a new campaign, which is the re-drafting of the rules of cyberspace global and reduce the growth of cyber threats and electronic defense, The Russian perspective of cyber warfare is clearly evident from its Western counterparts. This is evident in the way Russian theorists define cyber warfare, which refers to how Russia controls cyberspace to achieve the national goals of the Russian Federation. Where Russia is specialized in dealing with various challenges of electronic security and cyber threats, through the development of strategic plans to combat those threats and achieve national cyber security. Prompting Russia to impose a new doctrine of the existence of restrictions on services that are related to the means of media influence exercised by other countries aimed at destabilizing internal political and external Affairs in Russia.

جدول لأهم المصطلحات:

Terminologies in the English	المصطلحات اللغة العربية
Cyber Space	الفضاء السيبيري
Cyber Security	الأمن السيبراني
Cyber Infrastructure	بنية تحتية سيبرية
Cyber Threats	تهديدات سيبرانية
Cyber Attaks	هجمات سيبرانية
Cyber Power	القوة السيبيرية
Cyber Terrorism	الإرهاب السيبراني
Cyber Espionage	التجسس السيبراني
Cyber Crime	الجريمة السيبرانية
Cyber Diplomacy	الدبلوماسية السيبرانية
Cyber Intelligence	الاستخبارات السيبرانية
Cyber Deterrence	الردع السيبراني

جدول المختصرات:

اختصارها	الجملة بالانجليزية	الجملة بالعربية
NII	Nationalism Infrastructure Information	البنية التحتية القومية للمعلومات
ISS	International State Security	نظرية الدولة العالمية للأمن
UA	Universal Association	نظرية المجتمع العالمي للأمن

مقدمة

مقدمة

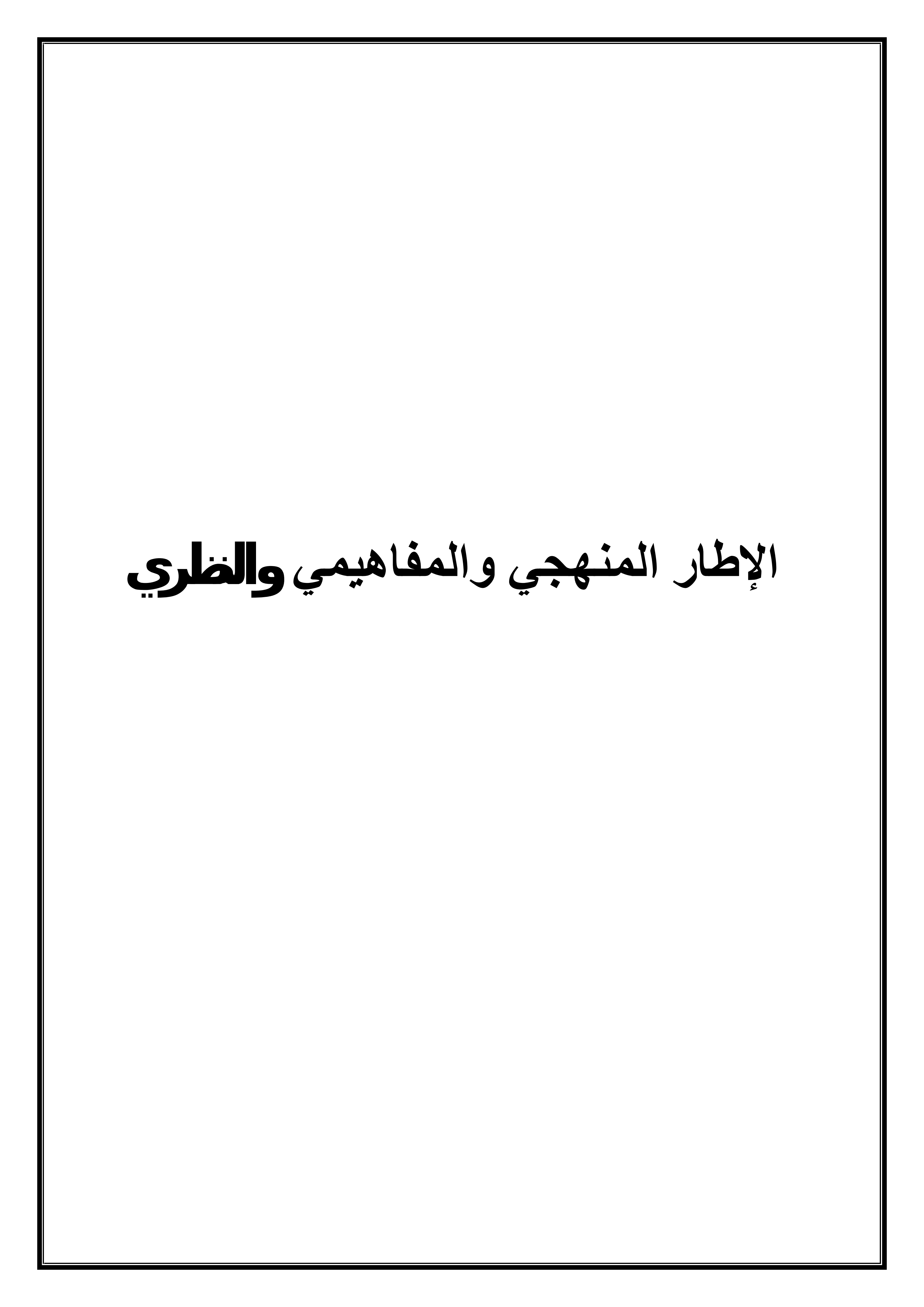
يشهد العالم اليوم مجموعة من التغيرات في الدراسات الأمنية، أثرت على مختلف المفاهيم وتطويرها إلى مفاهيم جديدة مواكبة للعصر، خاصة بعد نهاية الحرب الباردة، حيث تمثلت هذه التغيرات في توسيع مفهوم الأمن العسكري إلى مجالات غير عسكرية، حيث بات موضوع الأمن يركز على تفاعلات الظاهرة الأمنية مع تغيرها من الفواعل المهددة لها، لاسيما في منتصف القرن العشرين أين بدأ العالم يشهد إعادة تشكل القوى والفواعل المؤثرة في بنية النظام الدولي بشكل جعل من إدراك هذه التهديدات والمخاطر يدفع بالتحليل الأمني إلى الإنتقال من المستوى الدولاتي إلى مستويات أخرى غير دولاتية.

وأمام هذه الأوضاع الأمنية غير المستقرة التي يشهدها العالم اليوم، ومع تسارع التطورات التكنولوجية وظهور تقنيات حديثة للإتصالات وحركة تدفق المعلومات عبر الحدود الجغرافية بين الدول محولة بذلك العالم إلى قرية صغيرة فرضت واقعا جديدا على السيادة الوطنية، الأمر الذي ساهم في بروز مسألة جديدة تتمثل في مفهوم الأمن السيبراني، هذا المفهوم الذي ظهر نتيجة العلاقات التي تحاك عبر الفضاء الإلكتروني بين أشخاص موجودين على أراضي مختلفة.

حيث تحوّل الأمن السيبراني إلى ساحة التفاعلات الدولية من خلال العديد من الأنماط التوظيفية، سواء على الصعيد المدني أو العسكري، الأمر الذي جعل الفضاء السيبراني مجالا واسعا للصراعات المختلفة بين الدول.

وهو ما دفع روسيا إلى البحث في تعزيز مكانتها الدولية خاصة منذ وصول "فلاديمير بوتين" إلى السلطة سنة 2009 والذي يعتبر المنعرج المهم في تاريخ روسيا.

ولقد حاولت روسيا بقيادة "فلاديمير بوتين" رفع معدلات النمو في مختلف المجالات بوتيرة متسارعة لاستعادة مكانتها الدولية، فبرزت كدولة منافسة للولايات المتحدة الأمريكية على الساحة الدولية بحيث يلحظ الصعود من خلال التحكم في الفضاء السيبراني، حيث ضاعفت روسيا جهودها في المجال السيبراني من خلال العقيدة التي أقرّها الرئيس فلاديمير بوتين التي من شأنها تعزيز التصورات الإستراتيجية الروسية بخصوص التصدّي للهجمات السيبرانية والحفاظ على مصالح الأمن القومي الروسي من خلال التحكم في الفضاء السيبراني.



الإطار المنهجي والمفاهيمي والنظري

أولا : مشكلة الدراسة:

شهدت روسيا تدهورا في أوضاعها الداخلية والخارجية في مختلف الميادين بعد إنهيار الإتحاد السوفياتي، فحاولت منذ مطلع القرن الحادي والعشرين العمل على استعادة نفوذها ومكانتها كقوة عظمى في الساحة الدولية، وبزيادة عدد الدول الأجنبية التي لديها تأثير على الأمن العسكري الروسي والتكنولوجي مما جعلها تفرض عقيدة جديدة وذلك بوجود قيود على الخدمات التي تخص تطور المنظومة الأمنية في ظل البيئة الإستراتجية الروسية، من هنا نطرح الإشكال الذي يفرض نفسه في هذه الدراسة:

كيف ساهمت الإستراتجية الروسية الأمنية في مواجهة التهديدات السيبرانية في فترة فلاديمير بوتين 2009-2014؟

ومن خلال التساؤل المركزي تبلورت مجموعة من الأسئلة الفرعية، سنحاول في هذه الدراسة الإجابة عنها.

1- ما المقصود بالأمن السيبراني وما هي خصائصه وموضوعاته؟

2- ما هي المحددات الرئيسية المؤثرة في الأمن والدفاع الروسي؟

3- ما هو دور الإستراتجية الروسية في إرساء الأمن السيبراني، وهل ستنجح في خطتها الإستراتجية لمكافحة التهديدات السيبرانية؟

ثانيا: مجالات الدراسة:

1- المجال الجغرافي: يتحدد المجال المكاني لهذه الدراسة من خلال عنوان الموضوع والذي يتعلق بالدولة الروسية وتحديدا الأمن السيبراني.

2- المجال الزماني: يمتد المجال الزماني للدراسة من العام الذي شهد حكم بوتين أي عام 2009 إلى غاية عام 2014 التي تتعلق بالإستراتيجية الروسية في مواجهة التهديدات السيبرانية.

3- المجال الموضوعي: تعنى الدراسة معالجة موضوع بالغ الأهمية ألا وهو الإستراتجية الروسية كقوة عالمية في مواجهة التهديدات السيبرانية في عهد فلاديمير بوتين 2009-2014.

ثالثا: أهمية الدراسة.

1- الأهمية العلمية: يكتسب موضوع الدراسة أهمية علمية انطلاقا من المتغيرات المراد تحليلها وتوضيح أهم الخطط والإستراتجيات الروسية التي جاء بها بوتين وأولويات المنظومة الأمنية حيث باتت إشكالية التهديدات السيبرانية تحظى بدائرة.

اهتمام متزايد من طرف الباحثين والأكادميين بهدف فهم وتبسيط العقيدة الروسية في ما يخص التهديدات الموجهة للأمن العسكري والتكنولوجي في روسيا.

2- الأهمية العملية: أما عمليا فتهدف الدراسة إلى مدى يعيش هذا الوضع الراهن ومعرفة العلاقة بين الإستراتجية الروسية والتهديدات السيبرانية.

حيث تأتي الدراسة كإضافة لما سبق ولعل خصوصيتها تنبع من كونها تعالج الموضوع في ظل أهم المراحل التي تمر بها الدولة الروسية في الوقت الراهن لمجابهة االتهديدات السيبرانية.

3- الإقترابات:

- **الإقتراب الشخصي**: ينظمّ للظاهرة السيبرانية من خلال الإعتماد على نسق موجود في بيئة يتفاعل معها أخذا أو عطاءً حيث وضع "دايفيد إستون" عدة مفاهيم يمكن استخدامها في التحليل (مدخلات، المخرجات، التغذية المرجعية...) فهذه المفاهيم لها علاقة وطيدة بالموضوع وذلك مرده أن السياسة الأمنية الروسية هي عبارة عن مخرجات للنظام الأمني القائم.

- **الإقتراب الليبرالي**: يتحدد في تحاور الدول من أجل تحقيق المصالح والتكامل في العديد من المجالات الاقتصادية والعسكرية والاجتماعية، كما يدعوا إلى الإصلاح المؤسساتي خلال ذلك، التعاون الروسي التركي الروسي، الإيراني، الصيني.

- **الإقتراب الوظيفي**: يرى علماء السياسة الوظيفيون أن كل ما يترتب عن نشاط اجتماعي يؤدي إلى تكيف هذا النشاط مع بناء معين أو جرد من هذا البناء، حيث ينطبق هذا المقترب من نشاط المجتمع الروسي

المعلوماتي وتكيفه مع استخدامات الأنترنت وشبكات التواصل الإجتماعي، وما له من نتائج قد تنعكس على المنظومة الأمنية الروسية.[1]

رابعا:فرضيات الدراسة.

1- فرضية رئيسية: تنطلق الدراسة في فرضية رئيسية كإجابة مؤقتة على الإشكالية المطروحة.

تعد العقيدة الروسية الأفضل فيما يخص التهديدات الموجهة للأمن الروسي والتي تعمل بشكل مؤكد على الحماية من العمليات السيبرانية من قبل الأجهزة الخاصة الأجنبية.

2- الفرضيات الجزئية:

- تعدد مصادر التهديدات السيبرانية ساهم في تطور مستويات وأبعاد الأمن.

- انعكست المتغيرات التي تقدمها الساحة الروسية داخليا وخارجيا على توجيه الإستراتجية الروسية تجاه الأمن السيبراني.

خامسا: المناهج واقتراحات الدراسة:

I. مناهج الدراسة:

- **المنهج الوصفي التحليلي**: استخدمنا هذا المنهج كوظيفة لرصد وجمع المفاهيم والمصطلحات المرتبطة بالأمن والإستراتجية الأمنية وتحديد جوانب الظاهرة الأمنية والتهديدات السيبرانية وكذا وصف طبيعتها والتعرف على حقيقتها؛ كما اعتمدنا المنهج الوصفي التحليلي لتحديد الظروف والعلاقة بين المتغيرات.

- **المنهج التاريخي**: الإستعانة بأسلوب العرض الكرونولوجي المشتق من المنهج التاريخي من خلاله تم دراسة تطور العقيدة الأمنية الروسية عبر مسار تاريخي ارتبط بالتغيرات الحاصلة في مجال الظواهر الأمنية في فترة بوتين.

- **منهج دراسة الحالة**: هو المنهج الذي يتّجه إلى جمع البيانات العلمية لأيّ وحدة سواء كانت فردا أو مؤسّسة أو نظاما إجتماعيا أو مجتمعا محليا أو مجتمعا عاما، وهو يقوم على أساس التعمّق في دراسة مرحلة

---

[1]- عبد الغفار رشاد القصي، **مناهج البحث في علم السياسة**، (القاهرة: مكتبة الأردن، 2005)، ص 225.

معيّنة من تاريخ الوحدة أو دراسة جميع المراحل التي مرّت بها وذلك بقصد الوصول إلى تعميمات علمية متعلّقة بالوحدة المدروسة وبغيرها من الوحدات المشابهة لها.

وسيتم اعتماد هذا المنهج في الجزء التطبيقي من المذكرة أين سيتمّ إسقاط أجزاء من الإستراتيجية الروسية في مواجهة التهديدات السيبرانية وكذا كيفية إدارة القيادة الروسية بزعامة بوتين لهذه الإستراتيجية.

تحديد المصطلحات:

– **الإستراتجية**: **the stratégique**: يعد مصطلح الإستراتجية من المصطلحات الحديثة نسبيا لكن جذوره التاريخية تعود إلى فترة زمنية بعيدة، ويعود استخدامه إلى الإغريق الذين أعطوا لهذا المصطلح المضمون العسكري، وقد أصبح معروفا لمدة طويلة من الزمن أن الإستراتجية تعرف على أنها من كبار العسكريون أو من الأشياء العامة.[1]

أما الإستراتجية الأمنية فقد عرفت منحى متوافق مع تغير مفاهيم الأمن التي عرفت تراجع واضح للإستراتجية العسكرية من خلال التذبذب الواضح الذي ظهر على مستويات التسلح العسكري للدول.[2]

– **المنظومة الأمنية the system Security**: هي كل من يعمل في مجال الأمن ونظام تضعه أي منشأة لحماية محتوياتها.

– **التحديات الأمنية**: **challenges and Security:** هي تلك المشاكل أو الصعوبات أو الأخطار التي تواجه الدولة وتحد وتعوق من تقدمها وتشكل حجر عقبة أمام تحقيق أمنها واستقرارها ومصالحها الحيوية الذاتية والمشتركة ويصعب تجنبها أو تجاهلها قد تبدأ أو تنتهي بزوال أسباب بلوغ المفروض عليه التحدي دون الوصول إلى مرحلة التوازن يستغرق وقتا زمنيا أكبر من ذلك الوقت الذي يستغرقه التهديد.[3]

---

[1]– سعد شاكر شابي، **الإستراتجية الأمريكية تجاه الشرق الأوسط**، (عمان، مكتبة الحامد للنشر والتوزيع، 2013)، ص 13.

[2]– سمية طويل، **الإستراتجية الأمنية الأمريكية في منظمة شمال شرق آسيا، دراسة لما بعد الحرب الباردة**، (أطروحة دكتوراه، كلية العلوم السياسية جامعة الحاج لخضر، تخصص علاقات دولية، 2009–2010)، ص 38.

[3]– د. إدريس عطية، الإرهاب في إفريقيا دراسة في الظاهرة وآليات مواجهتها، رسالة ماجستير، جامعة الجزائر، ص 29.

– **الأمن السيبراني**: **cyber Security**: يتضمن تأمين البيانات والمعلومات التي تتداول عبر الشبكة الداخلية والخارجية من الاقتراحات الإلكترونية منها بشتى أنواعها، ويعتبر الأمن السيبراني هو السلاح الإستراتيجي الوحيد أمام الهجمات الإلكترونية وجزءا من تكتيكات الحروب الحديثة.[1]

II. المداخل النظرية:

النظرية الواقعية التي تركز على متغير القوة الذي من خلاله تهدف هذه الدراسة إلى الجهود الروسية في مجال تحقيق الأمن السيبراني لبعد جديد في السياسة الدفاعية الروسية.

– مدرسة كوبنهاجن: من خلال أمنية القضايا البيئية الرقمية والفضاء السيبراني بتشخيص التهديدات للدولة والمجتمع.[2]

III. أدبيات الدراسة:

حضى موضوع الإستراتجية الروسية لمكافحة التهديدات السيبرانية، الأمن السيبراني في عهد فلادمير بوتين باهتمام العديد من الدراسات أهمها:

1– دراسة قام بها شكلاط وسام، حول الإستراتجية الروسية في عهد بوتين من 2000 إلى 2014 دراسة حالة الجنوب المتوسط، وتهدف هذه الدراسة إلى فهم وتفسير السلوكات الخارجية الروسية في عهد فلاديمير بوتين التي تضمنتها الإستراتجية الشاملة للعودة الروسية للمسرح الدولي كقوة عظمى.

2– سعيدة رشاش، مكافحة الأمن السيبراني في منظومة الأمن الوطني الجزائري حيث تهدف هذه الدراسة لمعرفة العلاقة الترابطية بين الأمن الوطني والتهديدات السيبرانية (تأثير وتأثر) ما بات يعتم على الأجهزة الأمنية العماليّتية المختصة ضرورة تبني إستراتجيات وسياسات قطرية تهدف إلى التمكن من مكافحة هذه التهديدات.

---

[1]– فيصل يوسف، الأمن السيبراني والفضاء الإلكتروني، جريدة الموسم، السعودية شوهدت بتاريخ، 10.02.2019، رابط المقال:

htpp// www.alyaum.com/azlin

[2]– فريدة طاجين، سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية، واقع وتحديات، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية، ص 341.

دراسة لكل من "خالد سليمان" "أسماء الباهي" استراتيجيات الدول الكبرى في حماية أمنها الالكتروني (دراسة حالة: الولايات. م.أ) تهدف هذه الدراسة إلى:

- رصد أهم الثغرات النظرية والمخرجات الفكرية التي يمكن أن تساعدنا في التحول والتوسع في مفهوم الأمة.
- التعرف على أنجح النماذج الإستراتيجية لحماية أمن المعلومات.
- التعرف على الاستراتيجيات والوسائل التي تضمن القضاء على التهديدات الدبلوماسية.

الاتجاهات الجديدة في الدراسات الأمنية دراسة ل: "قسوم سليم" بعنوان "دراسة في تطور مفهوم الأمن عبر منظارات العلاقات الدولية" تحاول هذه الدراسة تحليل هذه النقلة النظرية بفحص ومقارنة المضامين النظرية لمختلف المفاهيم الأمنية كما لا يراد منها إيجاد وتعريف محدد للأمن بقدر ماهية محاولة للتوصل إلى بناء فكري متكامل أو إطار معرفي منسجم لما تعنيه كلمة "الأمن" في السياسة العالمية لنشره ما بعد الحرب الباردة.

مقال ل: "د.نورة شلوش" بعنوان "القرض الإلكتروني في الفضاء الليبرالي" "التهديد المضاعف لأمن الدول" والهدف منها: التعرف على الاستراتيجيات والآليات التي يمكن تفعيلها من قبل الأنظمة الدولية لتجديد الأمن الليبرالي الدولي ومعرفة مدى علاقة القرصنة الالكترونية بإحداث تغيرات في البيئة الأمنية السيبرانية الدولية والتعرف على تأثير الهجمات السيبرانية ومنها القرصنة الالكترونية في بروز أنماط جديدة للصراع الدولي.

الفصل الأوّل: التأصيل النظري والمفاهيمي السيبراني.

المبحث الأوّل: ماهية الأمن السيبراني والفضاء السيبراني.

المطلب الأوّل: مفهوم السيبرانية، والأمن السيبراني.

المطلب الثاني: الفضاء السيبراني؛ مفهومه، خصائصه وفواعله.

المطلب الثالث: أشكال تهديدات الأمن السيبراني.

المبحث الثاني: أنماط الحروب السيبرانية ومخاطر عسكرة الفضاء الالكتروني.

المطلب الأوّل: أنماط الحروب السيبرانية.

المطلب الثاني: مخاطر عسكرة الفضاء الالكتروني.

المبحث الثالث: نظريات وأبعاد ومداخل الأمن السيبراني.

المطلب الأوّل: نظريات الأمن ومستوياته.

المطلب الثاني: أبعاد الأمن السيبراني.

تمهيد:

يعتبر الأمن الركيزة الأساسية للمجتمع، بحيث لا يمكن تصور نمو أي نشاط بعيدا عن تحققه، سواء أكان ذلك، على المستوى التقني، أم على المستوى القانوني. وقد تحول الأمن، مع بروز مجتمع المعلومات، والفضاء السيبراني، إلى واحد من قطاع الخدمات، التي تشكل قيمة مضافة، ودعامة أساسية، لأنشطة الحكومات والأفراد، على السواء، كما هو الحال، مع التطبيقات الخاصة بالحكومة الالكترونية، والصحة الالكترونية، والتعليم عن بعد، والاستعلام، والتجارة الالكترونية، وغيرها الكثير. إلاّ أنّ الوجوه المتعددة للأمن السيبراني، ومضاعفاتها الخطيرة التي لا تقف عند حدود الإساءة إلى الأفراد، والمؤسسات، بل تتعداها إلى تعريض سلامة الدول والحكومات، تزيد مهمة القيمين على الموضوع تعقيدا وصعوبة، وتستدعي مقاربة شاملة ومتكاملة، لجميع التحديات، التي يطرحها الفضاء السيبراني، بحيث تأتي الردود، والحلول المقترحة، ناجعة وفاعلة.فتحقيق الأمن، وبناء الثقة في الفضاء السيبيري، من أساسيات تسخير تقنيات المعلومات والاتصالات في مجالات التنمية خدمة للمجتمعات الإنسانية.

المبحث الأوّل: ماهية الأمن السيبراني والفضاء السيبراني.

المطلب الأوّل: مفهوم السيبرانية، والأمن السيبراني.

أوّلا- السيبرانية لـغـة:

تذكر المراجع العلمية بأن عالم الرياضيات "نوربرت وينر Wiener Norbert" هو أوّل من استخدم مصطلح السيبرانية وذلك في عام 1948، في أثناء دراسته لموضوع القيادة والسيطرة والاتصال في عالم الحيوان، فضلاً عن حقل الهندسة الميكانيكية.[1]

أمّا فيما يتصل بالبحث عن مصدر كلمة سايبر (Cyber) في المعاجم اللغوية، فيتضح أنّها يونانية الأصل وترجع إلى مصطلح (Cybernetes)، الذي ورد بداية في مؤلفات الخيال العلمي ويعني القيادة أو التحكم عن بعد.

وما يؤكّد ما طرح سلفاً، إنّ معظم القواميس المتخصصة في المصطلحات العسكرية، لم ترجع كلمة سايبر إلى مصدرها، بل عرّفت في نطاق استخدامها الفعلي أي العسكري، كقاموس المصطلحات العسكرية الأمريكية إذ يعرفها: "أيّ فعل يستخدم عن طريق شبكات إلكترونية بهدف السيطرة أو التعطيل لبرامج الكترونية أخرى".[2]

فيما عرف معجم مصطلحات الكمبيوتر والمعلوماتية، السيبرانيات بأنّها: "علم التحكّم والإتّصال، علم المراقبة والإتّصال".[3]

أمّا في اللغة العربية وبالرجوع إلى المختصين فيها، فنجد أنّ تحدياً يواجهونه في اختيار مصطلح مقارب لمصطلح (Cyber) في اللغة الانجليزية، ولا أدّل على ذلك من أنّ الترجمة العربية لعنوان اتفاقية مجلس أوربا

---

[1]– أحمد عبيس نعمة الفتلاوي، **الهجمات السيبرانية؛ مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر**، (العراق: مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، 2016)، ص 04.

[2]– نفس المرجع، ص 04.

[3]– إ.و. حدّاد، **معجم مصطلحات الكمبيوتر والمعلوماتية إنجليزي – فرنسي – عربي**، (لبنان: مكتبة لبنان، د.ت)، ص 74.

المتعلقة بالجريمة السيبرانية كانت ترجمة غير صائبة، إذ تُرجِم العنوان (Convention on Cyber crime) إلى اللغة العربية (الإتفاقية المتعلقة بالجريمة الإلكترونية) ويعود السبب في ذلك إلى عدم وجود مصطلح مناظر في اللغة العربية.[1]

ثانيا- السيبرانية اصطلاحا:

تعني ترابط الحواسب مع أنظمة أوتوماتيكية، والنظم الإلكترونية المركزية بتنسيق كل الآلات والمعدات التي تستخدم على نطاق المدينة، الأمّة والعالم بشكل شامل، لتحقيق أعلى رفاهية للبشر جميعا ويمكن للمرء أن يفكر بهذا كنظام إلكتروني عصبي، لا إداري يمتد في كل مناطق التركيبة الإجتماعية.[2]

ثالثا- تعريف الأمن السيبراني:

يمكن تعريف الأمن السيبراني، انطلاقا من أهدافه، بأنّه النشاط الذي يؤمن حماية الموارد البشرية، والمالية، المرتبطة بتقنيات الإتصالات والمعلومات، ويضمن إمكانات الحد من الخسائر والأضرار، التي تترتب في حال تحقق المخاطر والتهديدات، كما يتيح إعادة الوضع إلى ما كان عليه، بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج، وبحيث لا تتحول الأضرار إلى خسائر دائمة. فهو النشاط أو العملية، والقدرة، أو نظم المعلومات واتصالات الدولة، حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف، والاستخدام غير المصرح به أو التعديل، أو الاستغلال.[3]

ومن الناحية العملية الإجرائية يمكن تلخيص الأمن السيبراني على أنه لا يتعدى المفاهيم التالية:[4]

- "يتكون الأمن السيبراني إلى حد كبير من وسائل دفاعية تستخدم لكشف وإحباط المتسللين".

---

[1]- أحمد عبيس نعمة الفتلاوي، مرجع سابق، ص 04.

[2]- الموقع الإلكتروني: https://ar-ar.facebook.com/zeitgeist.arabic/posts/cybern/، "**ما هي السيبرانية؟ وما دورها في صناعة القرار؟**، تاريخ الإطّلاع: 2019/03/17، على الساعة: 19:45.

[3]- بارة سمير، **الأمن السيبراني (cyber Security) في الجزائر السياسات والمؤسسات**، (الجزائر: المجلة الجزائرية للأمن الإنساني، عدد الرابع، جامعة قاصدي مرباح - ورقلة، 2017)، ص 257.

[4]- نفس المرجع، ص ص 257 - 258.

- "الأمن السيبراني ينطوي على حماية شبكات الكمبيوتر والمعلومات التي تحتويها من الاختراق ومن الضرر الخبيث أو التعطيل".

- "الأمن السيبراني ينطوي على الحد من هجوم المخاطر الخبيثة على البرمجيات وأجهزة الكمبيوتر والشبكات. وهذا يشمل الأدوات المستخدمة للكشف عن اقتحام ووقف الفيروسات، ومنع وصولها، وفرض التوثيق، وتمكين الاتصالات المشفرة".

- "الأمن السيبراني هو مجموعة من الأدوات والسياسات والمفاهيم الأمنية، والضمانات الأمنية، والمبادئ التوجيهية، من المخاطر المحدقة بالمعلومات ومعالجتها، والإجراءات، والتدريب، وأفضل الممارسات، وضمان التقنيات التي يمكن استخدامها لحماية البيئة الإلكترونية وتنظيم أصول المستخدم".

- "القدرة على الحماية أو الدفاع عند استخدام الفضاء الإلكتروني من الهجمات السيبرانية".

- "الهيئة التكنولوجيات والعمليات والممارسات وتدابير الإستجابة والتخفيف، والتي تهدف إلى حماية الشبكات وأجهزة الكمبيوتر والبرامج والبيانات من هجوم أو التلف أو الوصول غير المصرح به وذلك لضمان توافر السرية والنزاهة".

- "فن ضمان وجود واستمرارية مجتمع المعلومات للأمّة، وضمان وحماية فضاء الإنترنت، والمعلومات الخاصة به، والأصول والبنية التحتية الحيوية".

- "حالة محمي ضد الجرم أو الاستخدام غير المصرح به للبيانات الإلكترونية، أو التدابير المتخذة لتحقيق ذلك".

ولا شك بأن الوصول إلى تعريف يتصف بالشمولية للأمن السيبراني يستدعي منا الوقوف عند مجموعة من العناصر تعد الفاعلة والمتحكمة في تحقيقه وهي: التكنولوجيا - الأحداث – الإستراتيجيات والعمليات والأساليب – الإنسان – المرجع الأمني.

وبالتمعن في هذه العناصر نتوصل إلى أنّ الأمن السيبراني يجب أن يتميز بـ:[1]

[1]- بارة سمير، مرجع سابق، ص 258.

– طابع متعدد التخصصات الإجتماعية والتقنية؛

– كونه شبكة خالية من الحجم، والتي قدرات الفاعلين يمكن أن تكون مماثلة على نطاق واسع؛

– درجة عالية من التغيير، الترابط وسرعة التفاعل؛

نخلص إلى أن الأمن السيبراني هو عبارة عن برامج وآليات تقنية، وقدارت بشرية تُفعل لمواجهة أيّ تعدي على المعلومات الإلكترونية بشتى أنواع الجريمة الإلكترونية.

المطلب الثاني: الفضاء السيبراني؛ مفهومه، خصائصه وفواعله.

الفرع الأوّل: مفهوم الفضاء السيبراني.

الفضاء السيبراني مجال إفتراضي من صنع الإنسان يعتمد على نظم الكمبيوتر وشبكات الانترنيت وكمّ هائل من البيانات والمعلومات والأجهزة.

يُتداول مصطلح "الفضاء السيبراني" أو كما يسميه البعض "الفضاء الإلكتروني" على أكثر من صعيد، ذلك كونه أساسا فضاءا اجتماعيا للتواصل والتبادل، إلَا أنَه أضحى مجالا حيويا وجيواستراتيجا تُخاض فيه العديد من الحروب والهجمات الرقمية.[1]

حيث عرَفته الوكالة الفرنسية لأمن أنظمة الإعلام (ANSSI)، وهي وكالة حكومية مُكلفة بالدفاع السيبراني الفرنسي على أنَه: "فضاء التواصل المشكَل من خلال الربط البيني العالمي لمعدات المعالجة الآلية للمعطيات الرقمية"[2].

كما جاء تعريف الاتحاد الدولي للاتصالات للفضاء السيبراني بأنّه " المجال المادي وغير المادي الذي يتكون وينتج عن عناصر هي: أجهزة الكمبيوتر، الشبكات، البرمجيات، حوسبة المعلومات، المحتوى، معطيات النقل والتحكم، ومستخدمو كلّ هذه العناصر"[1]

---

[1]– قادير إسماعيل، **إدارة الحروب النفسية في الفضاء الالكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط**، ندوة دولية بعنوان: عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية، (الجزائر: كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، 2019/02/12)، ص 04.

[2]– قادير إسماعيل، مرجع سابق، ص 04.

كما أنّ عملية تعزيز الجانب الدلالي لهذا الفضاء تستدعي تحليل البنية التركيبية له، إذ يُمكن اعتبارها بنية ذي ثلاث طبقات هي:[2]

1- الطبقة المادية: تشمل معدات الحواسيب، والبرمجيات، والمعدات الضرورية لعملية الربط البيني.

2- الطبقة المنطقية: تشمل مجموع البرامج المترجمة للمعلومة على شكل معطيات رقمية، حيث يتم الانتقال من لغة الإنسان إلى لغة الآلة في شكل خوارزمية، ومنها إلى برامج مطوَرة بلغة البرمجة.

3- الطبقة الإعلامية: وتتمثل هذه الطبقة في البُعد الاجتماعي الذي يُضاف إلى الطبقتين السابقتين، حيث أنه في الفضاء الرقمي يُمكن أن يكون لكل إنسان عدة هويات رقمية (عنوان بريده الالكتروني، رقم هاتفه النقال، صور رمزية على مواقع التواصل الاجتماعي...).

الفرع الثاني: خصائص وفواعل الأمن السيبراني.

أوّلا- الخصائص.

أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم،والتي تشمل الطاقة والاتصالات والنقل والخدمات الحكومية والتجارة الإلكترونية والمصارف والمؤسسات المالية، وحيث جعل الفضاء الإلكتروني من تلك المصالح مرتبطة ببعضها البعض في بيئة عمل واحدة والتي تعرف بالبنية التحتية القومية للمعلومات (NII) ومن ثم فإن أي هجوم على إحدى تلك المصالح أو كلها يمثل سببًا ومدعاة لحدوث عدم توازن استراتيجي بما يكشف في الوقت نفسه عن شكل جديد من أشكال الصراع ونمط جديد من التهديد للأمن القومي.[3]

---

[1]- The International Télécommunication Union, ITU Tool kit for Cybercrime Législation, Geneva, 2010, P 12.

[2]- لطفي لمين بلفرد، <u>**الفضاء السيبراني: هندسة وفواعل**</u>، (المجلة الجزائرية للدراسات السياسية، ENSSP، العدد الخامس، الجزائر، 2016)، ص ص 148-150.

[3] -Richard K. Betts.*Conflict after the Cold War*, <u>***Arguments on Causes of War and Peace*, 2nd ed**</u>. (New York: Longman, 2002), P 548-557.

وساعد في ذلك عدد من التحولات لعل أهمها، ارتباط العالم المتزايد بالفضاء الإلكتروني ممّا أدّى إلى زيادة خطر تعرض البنية التحتية الكونية للمعلومات لهجمات إلكترونية. واستخدام الفاعلين من غير الدول للفضاء الإلكتروني لتحقيق أهدافهم وتأثير ذلك على سيادة الدولة. وانسحاب الدولة من قطاعات استراتيجية لصالح القطاع الخاص وخاصة بالمنشآت الحيوية.وتأثير مواجهة الحرب الإلكترونية على حرية استخدام الفضاء الإلكتروني.[1]

إشكالية تعامل الدول مع الشركات التكنولوجية متعدية الجنسيات والتي أصبحت تفوق قدراتها بعد أن أصبحوا فاعلين دوليين.

وكان للفضاء الإلكتروني دور في وجود أهداف ووسائل ومصالح إلكترونية جديدة، وفي نفس الوقت أتاح القابلية لخطر التعرض للهجوم، وهو ما أوجد نوعًا جديدًا من الضرر دون الحاجة للدخول الطبيعي والمادي لإقليم الدولة، وذلك لاعتماد الدول على الأنظمة الإلكترونية في كافة منشآتها الحيوية بما يجعل من تلك الأنظمة هدفًا للهجوم، خاصة وأنّ تلك الأنظمة تحمل طابعًا مدنيا وعسكريًا مزدوجًا. وذلك بعد أن تمخض عن الثورة التكنولوجية ثورة أخرى هي الثورة في الشؤون العسكرية وتطور تقنيات الحرب.

وتتميز الحروب السيبرانية بأنها قليلة التكلفة، فقد يتم شن حرب بتكلفة دبابة عبر أسلحة جديدة ومهارات بشرية، ويتم استخدامها في أي وقت، سواء أكان وقت سلم أم حرب أم أزمة. ولا تتطلب لتنفيذها سوي وقت زمني محدود، وتعد تكلفة إطلاق تلك الهجمات أقل من أي سلاح تقليدي آخر.

وتعد الحرب الالكترونية جزءا من عمليات المعلومات المستخدمة في مستويات ومراحل الصراع المختلفة، سواء كان ذلك علي الجانب التكتيكي أو الاستراتيجي أو العملياتي بهدف التأثير بشكل سلبي في المعلومات ونظم عمله، واستخدام الفضاء الإلكتروني لإيجاد ميزة أو تفوق أو تأثير في البيئات المختلفة وعبر أدوات القوة ، ومن أهم المتغيرات هو ظهور الاستراتيجية السيبرانية والتي تشير إلى القدرة على التنمية وتوظيف القدرات للتشغيل في الفضاء الإلكتروني مندمجة وبالتنسيق مع المجال العملياتي الآخر لتحقيق أو دعم إنجاز الأهداف عبر عناصر القوة القومية.

---

[1]- **عادل عبد الصادق، الحروب السيبرانية : تصاعد القدرات والتحديات للأمن العالمي، (**المركز العربي لأبحاث الفضاء الإلكتروني، 2017/03/12)، متاح على الرابط: http://accronline.com/print_article.aspx?id=28395.

ثانيا- الفواعل.

يمكن تقسيم الفواعل في الفضاء السيبراني ومن لديهم القدرة على شن الهجمات الالكترونية إلى ما يلي:

1- الدولة:

تمثل الخطر الأكثر والفاعل قوة في مجال الفضاء السيبراني، فهي نهاية عام 2008، استطاعت حوالي 180 دولة أن تمتلك ترسانة من الأسلحة الالكترونية، مما قد يدفع الفواعل من الدول ومن غير الدول للتنافس في السنوات القادمة من أجل تحقيق التفوق الإلكتروني. ونتيجة لما يقدمه الفضاء السيبراني فرض الفواعل لتحقيق مصالحهم، تسعى عديد من الدول إلى تطوير قدرتها في هذا المجال، وتنقسم القدرات السيبرانية للدول بشكل عام إلى قدرات دفاعية وأخرى هجومية، ولكن أضاف كل من "**ريتشارد كلارك**" (Ritchard Clarke) و"**روبرت كناك**" (Robert Knake)[1]، في كتابيهما عن الحرب الإلكترونية باعتبارها الخطر القادم الذي يهدد الأمن القومي للدول. ويعتبر بعدا آخر يرتبط بمدى اعتماد الدول في الفضاء السيبراني لإدارة شؤون الدولة، فقدرة الدولة تزيد كلما زادت قدراتها الهجومية والدفاعي، وقل اعتمادها نسبيا على الفضاء السيبراني مقارنة بغيرها من الفواعل.[2]

2- الفواعل من غير الدول:

إن تصاعد خطر الفاعلين من غير الدول على الأمن السيبراني في العلاقات الدولية قد أثر بدوره على سيادة الدول، وبخاصة مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية وبروز أخطار القرصنة والجريمة الإلكترونية والجماعات الإرهابية، ومن جهة أخرى فقد فرض ذلك تحدي الحفاظ على الأمن دون إشراك هؤلاء الفاعلين الجدد في تحمل المسؤولية والعبء في تأمين البنية التحتية المعلوماتية وبدأ يظهر اتجاه التعددية في

---

[1]– نوران شفيق، **أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني**، (القاهرة: المكتب العربي للمعارف، 2014)، ص 40.

[2]– نوران شفيق، **أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني**، مرجع سابق، ص 40.

الحفاظ على الأمن بين كافة أصحاب المصلحة من الحكومات والمجتمع المدني والقطاع الأكاديمي والتقني والقطاع الخاص ووسائل الإعلام.[1]

إن ظهور الأطراف الجدد من غير الدول في تزايد مستمر، فعبور نشاطات هذه الأطراف للحدود جعل التفاعلات الدولية أكثر تعقيدا، حيث أفرزت هذه الأطراف أنماطا جديدة من المشكلات والمنازعات، فقد ساهمت هذه التنظيمات في (خصخصة الحرب وأصبحت تساهم في التدريب والتجنيد والحوار...الخ). وبرزت مشكلات الحروب الفضائية التي تمثل الفيروسات بخسائر وصلت إلى حوالي 15 مليار دولار، كما أن جماعات الجريمة المنظمة كلفت من خلال انتهاكات للملكية الفكرية وسرقة البيانات حوالي تريليون دولار في عام 2008، كما أن شبكات التجسس الإلكتروني اقتحمت 1295 حاسوبا في 103 دولة منها 30% أهداف حكومية مهمة.

3- الفرد:

أضحى الفرد فاعلا مهما في الفضاء السيبراني، حتى أن له القدرة على إحداث ثورة الرقمية، لتصبح تلك الثورة مجال استخدام للدولة نفسها، ومثال ذلك ما قام به "**مارك زوكربارغ**" (Mark Zoukberg) عام 2004، حين أسس الـ (facebook)، لتستقطب أكثر من مليار مستخدم عبر العال. وغيرها من وسائل التواصل الاجتماعي بمختلف أنواعها، حيث تبقى هذه الوسائل بحرا لحرية الأفراد الذين يمارسون نوعا من المعارضة الإفتراضية، إلا أن هذا الجانب من الحرية أعطى الوقت للأفراد على اختلاف توجهاتهم وانتماءاتهم سواءا كانوا رسميون أو غير ذلك، فسحة واسعة لنشر الأفكار والمعلومات سواء كانت سليمة أو ضارة بالآخرين، يبقى هنا يجب أن يتحلى الأفراد من وعي كاف كي يميز بين هذه الصفحات الإلكترونية ويبني مقاربة ثقافية توعوية.[2]

---

[1]– عادل عبد الصادق، **خطر الحروب السيبرانية" عبر الفضاء الإلكتروني**، (مصر: مجلة الأهرام لكمبيوتر الانترنت والاتصالات، مارس 2017)، ص27.

[2]– قادير إسماعيل، مرجع سابق، ص 05.

4- المجموعات الإفتراضية (Virtual Community):

تتخذ هذه المجموعات سمات متميزة تجعلها فضاءا مثاليا للتواصل، خاصة بالنسبة إلى الأجيال الشابة التي أضحت الثقافة الرقمية المرتكزة على الصورة تشغل حيزا مهما من حياتها بكل ما تحمله من رموز ودلالات، وقواعد التواصل والتبادل، وعلاقات إجتماعية وغيرها، فالمجموعات الإفتراضية حسب "**هاورد رينغولد**" (Hawrd Rengold) وهي مجموعات تنشأ من الشبكة حين يستمر أناس بعدد كاف من الزمن لتشكيل علاقات شخصية في الفضاء السيبيري. أما البحث الإجتماعي "**نديم منصوري**"، فيرى أنها مجموعة من الأفراد يتشاركون عبر الانترنت لفترة زمنية، لتحقيق غاية أو هدف أو هواية، من خلال علاقة إجتماعية إفتراضية تحددها منظومة "**تكنو– إجتماعية**". فتتحقق المجموعات الإفتراضية من خلال بروزه كفاعل أو متفاعل أثناء عمليات التواصل عبر الشبكة، وتختلف هذه المجموعات حسب هوياتها حسب الباحثة الفرنسية "**فاني جورج**" (Vanny Gzorges) وهي الآتي:[1]

الهوية التصريحية (**Identité déclarative**): تبرز من خلال المعلومات التي يجرى إدخالها من قبل صاحب الحساب.

هوية ثنائية القطب (**Diasporiens Bipolaires**): تضم أقلية تعبر عن ارتباطها العميق في الوقت ذاته بالوطن الأم والبلد والمستقبل.

هوية عالمية (**Les Cosmopolites**): تعرض انفتاحا على مختلف الثقافات العالمية، وتشير الباحثة إلى أن هذه المجموعات لا تخفي حقيقة التغيرات والممارسات الهوياتية بفعل سهولة التواصل والتفاعل عبر الفضاء السيبراني.

---

[1]– كلثوم بيبيمون، **السياقات الثقافية الموجهة للهوية الرقمية في ضوء تحديات المجتمع الشبكي من التداول الافتراضي إلى الممارسات الواقعية**، (بيروت: مجلة "إضافات"، مركز دراسات الوحدة العربية، العدد 23، 2016)، ص 26.

المطلب الثالث: أشكال تهديدات الأمن السيبراني.

تتعدد أشكال الهجمات الإلكترونية التي يتم فيها استخدام الأسلحة، وإن كانت الأهداف الكامنة وراء عدد كبير من هذه الهجمات هي أهداف تقليدية كالتجسس وسرقة المعلومات وشن الحروب والتي بات عديدٌ من الفواعل الدوليين يلجئون إلى آليات إلكترونية لتحقيقها. وعلى الرغم من تعدد صور وأشكال الهجمات الإلكترونية، غير أنه من الممكن تقسيمها إلى أربع مجموعات رئيسية نوضحها كالتالي:[1]

أوّلا- التجسس الإلكتروني.

التجسس الإلكتروني (cyber espionage) هو القيام باختراق شبكة أو جهاز إلكتروني بهدف سرقة المعلومات الموجودة عليه، والتي عادة ما تكون على درجة كبيرة من الأهمية، سواء أكانت معلومات عسكرية أم اقتصادية أم صناعية أم تجارية أم غيرها، وهو ما يترتب عليه آثارٌ استراتيجية فادحة في الطرف المستهدف. فلقد غيرت التطورات التكنولوجية في العصر الحديث من طبيعة عمليات التجسس التقليدية، إذ توفر الآليات الإلكترونية والإنترنت فرصًا جديدة أقل تكلفة وأقل خطورة للفواعل من الدول وغير الدول للقيام بعمليات التجسس.[2]

وتوضح عديدٌ من التقارير أنّ عمليات التجسس الإلكتروني في تزايد مستمر، فوفقًا لأحد التقارير الأمنية الصادرة عن شركة آي بي إم (IBM) بلغ عدد عمليات التجسس الإلكتروني حوالي 237 مليون حالة على مستوى العالم في الستة أشهر الأولى من عام 2005. وأظهر التقرير أن المؤسسات الحكومية هي الأكثر عرضة للتجسس الإلكتروني، كما تأتي الولايات المتحدة على قمة قائمة الدول التي تتعرض لهذا النوع من الهجمات. ففي النصف الأول من عام 2005 تعرضت الولايات المتحدة لأكثر من 12 مليون هجوم إلكتروني بغرض التجسس. وتأتي في المرتبة الثانية في العام ذاته نيوزلندا (2،1 مليون هجوم)، والصين (مليون هجوم).[3]

---

[1]– نوران شفيق، **أثر التهديدات الإلكترونية على العلاقة الدولية**، (القاهرة: المكتب العربي للمعارف، 2016)، ص 29.

[2]– نفس المرجع، ص 30.

[3]– نوران شفيق، **أثر التهديدات الإلكترونية على العلاقة الدولية**، مرجع سابق، ص 30.

ولأنّ هذه الهجمات تستطيع إحداث خسائر كبيرة في وقت محدود، أصبحت عديدٌ من الدول تلجأ إليها، إمّا في خلال أوقات النزاعات السياسية والتوتر السياسي مع دول أخرى، وإمَّا في وقت الحروب بالتزامن مع العمليات العسكرية التقليدية. ومن أبرز أمثلة التجسس الإلكتروني الذي تقوم به دول ضد أخرى هو ما ورد في تقرير لجنة التحقيقات التي شكلها البرلمان الأوروبي في عام 2001 والذي اتهم الولايات المتحدة باستخدام شبكة تجسس إلكترونية تحت اسم (Echelon network) تأسست في أثناء الحرب الباردة للتجسس وسرقة المعلومات الصناعية الخاصة بالصناعات الأوروبية.[1]

ثانيا- الجرائم الإلكترونية.

على الرغم من محورية مصطلح الجريمة الإلكترونية (cyber crime) في عديدٍ من الدراسات الأكاديمية التي تتناول التهديدات الإلكترونية في العصر الحديث، إلا أنه لا يوجد اتفاق على تعريف محدد لماهية الجريمة الإلكترونية وعناصرها وأشكالها. ولكن بصفة عامة، يمكن تعريف الجريمة الإلكترونية على أنها تلك الجريمة التي يتم فيها استخدام الآليات والأسلحة الإلكترونية السابق ذكرها للقيام بهجوم إلكتروني بهدف تحقيق مكاسب مالية بالأساس.[2]

فلقد وفّرت التطورات التكنولوجية الحديثة مجموعة من الآليات التي يتمكن من خلالها الأفراد من القيام بالجرائم بتكلفة ومخاطر أقل. ومن ثم أصبحت الجرائم التقليدية تتم في صورة إلكترونية على نطاق واسع دون أن يكون هناك رادع أو آلية للعقاب، كما هو الحال في التعامل مع الجرائم الإلكترونية. وأدّى ذلك إلى ارتفاع معدلات الجرائم الإلكترونية بصورة كبيرة وخاصة مع زيادة عدد مستخدمي الإنترنت واعتماد الأفراد والمنظمات والدول عليه بشكل متزايد. فعلى سبيل المثال، قدرت الخسائر المترتبة على الجرائم الإلكترونية بالنسبة للأفراد حوالي 3،1 مليار جنيه إسترليني سنويًا، والخسائر الاقتصادية التي تتكبدها الحكومات حوالي 2،2 مليار جنيه إسترليني سنويًا، و21 مليار جنية إسترليني للقطاع الخاص سنويًا أيضًا.

وتتعدد أشكال الجرائم الإلكترونية التي يتعرض لها الأفراد والمنظمات والدول، ونوضح أهمها كالتالي:[3]

---

[1]- نفس المرجع، ص 30 – 31.

[2]- نوران شفيق، **أثر التهديدات الإلكترونية على العلاقة الدولية**، مرجع سابق، ص 31 – 32.

[3]- نوران شفيق، **أثر التهديدات الإلكترونية على العلاقة الدولية**، مرجع سابق، ص 33 – 34.

1- سرقة الهوية:

من أبرز أشكال الجرائم الإلكترونية وأكثرها خطورة هي جرائم سرقة الهوية (identity theft) وتشير سرقة الهوية إلى تلك العمليات التي يتم من خلالها سرقة معلومات شخصية عن الهوية تستخدم للاحتيال والقيام بأعمال غير قانونية واستغلال هذه المعلومات لتحقيق مكاسب مالية.() فعند إصابة جهاز الحاسب الآلي بأحد البرامج الخبيثة، قد يقوم هذا البرنامج بالبحث في الجهاز عن بيانات شخصية، مثل الاسم أو العنوان أو مكان الميلاد أو رقم الهاتف أو رقم بطاقة الهوية أو أرقام بطاقات الائتمان، إلى آخره من معلومات، ثم يتم استخدامها في تزوير بطاقات الهوية وشهادات ميلاد وكشوف حسابات البنوك وسرقة الأموال.

2- هجمات الاختراق:

هجمات الاختراق (penetration attacks) هي تلك الهجمات التي يتم من خلالها الدخول غير المشروع إلى الأنظمة الآلية وتخطي نظام التأمين الخاص بها. وفى حالات الاختراق الكامل يتمكن المهاجم من السيطرة الكاملة على الحاسب الآلي، وتغيير البيانات أو تبديلها، أو زرع برامج خبيثة داخل الجهاز.

وفى بعض الحالات يقوم المخترق (intruder) باستخدام الحاسب الآلي الذي تم اختراقه كأداة لشن هجوم إلكتروني على جهاز آخر خاصة وإن كانا متصلين بشبكة واحدة. يتطلب هذا النوع من الهجمات جمعُ معلومات حول النظام أو الشبكة التي سيتم اختراقها، والتعرف على أنظمة التأمين والتشغيل الخاصة بها، ومحاولة استغلال نقاط الضعف فيها وذلك لتسهيل اختراقها.

3– الاحتيال عبر الإنترنت:[1]

الاحتيال عبر الإنترنت Internet fraud هو نوع من الاحتيال يتم فيه استخدام الإنترنت ووسائطه المختلفة كالمواقع الإلكترونية والبريد الإلكتروني للقيام بعمليات احتيالية لتحقيق مكاسب مالية. وبسبب تزايد أعداد المستخدمين للإنترنت على مستوى العالم، ازدادت مخاطر تعرض الأفراد والشركات والمنظمات والحكومات لعمليات الاحتيال عبر الإنترنت.

[1]– نوران شفيق، **أثر التهديدات الإلكترونية على العلاقة الدولية**، مرجع سابق، ص 35.

وتتعدد أشكال جرائم الاحتيال عبر الإنترنت ومن أهمها القيام ببيع سلع وهمية (rogue traders) أو سرقة معلومات البطاقات الائتمانية واستخدامها (credit card fraud)، أو توجيه المستخدم إلى موقع خاطئ الغرض منه التحايل (pharming)، أو الاصطياد الاحتيالي (phishing) والذي يتعرض فيه الأفراد للخداع عن طريق توجيههم إلى مواقع يتم فيها الحصول على أكبر قدر من المعلومات الخاصة بهم، ثم استخدامها من قبل القائم بالجريمة لتحقيق مكاسب مالية.

المبحث الثاني: أنماط الحروب السيبرانية ومخاطر عسكرة الفضاء الالكتروني .

المطلب الأوّل: أنماط الحروب السيبرانية.

أوّلا- نمط "الحرب "الباردة الالكترونية والصراع "منخفض الشدة".

يتم استخدام الفضاء الإلكتروني كساحة للصراع منخفض الشدة،ويأتي هذا النمط ليعبر عن صراع ذو طبيعة ممتدة ومستمرة ودائمة النشاط العدائي أو غير السلمي، ويعبر هذا النمط عن صراعات أخرى أعمق وممتدة ذات نواحي ثقافية أو اقتصادية أو اجتماعية. ويتم استخدام نمط"القوة الناعمة "، ويتميز هذا النمط

بدرجة كبيرة من التعقيد والتداخل في معركة لا نهاية لها،ما بقيت الأبعاد الأخرى للصراع، ولا يتطور هذا النوع من الصراعات بالضرورة إلى حالة استخدام القوة المسلحة بشكلها التقليدي أو من خلال شن حرب إلكترونية واسعة النطاق.وتتم "الحرب الباردة الإلكترونية" من خلال شن الحرب النفسية والاختراقات المتعددة والتجسس وسرقة المعلومات وشن حرب الأفكار، ولا ترقى لعمل عسكري عنيف، أو من خلال انعكاس التنافس العالمي بين الشركات التكنولوجية والنفوذ ما بين أجهزة الاستخبارات الدولية، وهو ما يتم في حالات الصراع السياسي ذو البعد الاجتماعي- الديني الممتد، مثل: حالة الصراع العربي الإسرائيلي أو الصراع ما بين الهند وباكستان أو ما بين كوريا الجنوبية والشمالية، والصراع ما بين مناطق الصراع التاريخية.[1]

والى جانب ذلك تنشط جماعات دولية للقرصنة للتعبير عن مواقف سياسية أو حقوقية مثل جماعة "ويكيليكس" و"أنونيموس". أو في حالات الأزمات الدولية.[2]

ثانيا- نمط "الحرب" الالكترونية متوسطه الشدة.

يتحول الصراع عبر الفضاء الإلكتروني إلى ساحة موازية لحرب تقليدية دائرة، ويكون تعبيراً عن حدَّة الصراع القائم بين الأطراف، وقد يكون مقدمة لعمل عسكري. وتدور حرب عبر الفضاء الإلكتروني عن طريق اختراق المواقع وقصفها وشنِّ حرب نفسية وغيرها. ويستمد ذلك الصراع سخونته من قوة أطرافه وارتباطه بعمل عسكري تقليدي. وبخاصة مع تكلف فقط 4% من تكلفة الآلة العسكرية، بما يمكّن من تمويل حملة حربية كاملة عبر الإنترنت بتكلفة دبابة. كما أنّها لا تستغرق إلا وقتًا بسيطًا.[3]

ثالثا- نمط الحرب الالكترونية "الساخنه "والصراع مرتفع الشدة.

على الرغم من أنّ العالم لم يشهد حربا الكترونيا منفردة ودون العمل العسكري التقليدي إلاّ أنّ هناك إرهاصات لتحول ذلك في المستقبل. ويتميز هذا النمط من الصراع على سيطرة البعد التكنولوجي على إدارة العمليات الحربية حيث يتم استخدام الأسلحة الإلكترونية فقط ضد منشآت العدو، ويتم استخدام الروبوتات

---

[1]- عادل عبد الصادق، **الحروب السيبرانية؛ تصاعد القدرات والتحديات للأمن العالمي**، (إ.ع.م دبي: المركز العربي لأبحاث الفضاء الإلكتروني، 2017) متاح على الرابط: http://accronline.com/article_detail.aspx?id=28395.

[2]- نفس المرجع.

[3]- عادل عبد الصادق، **الحروب السيبرانية؛ تصاعد القدرات والتحديات للأمن العالمي**، مرجع سابق.

الآلية في الحروب والتي يتم إدارتها عن بعد فضلاً عن الطائرات بدون طيار، ويتم تطوير القدرات في مجال الدفاع والهجوم الإلكتروني والاستحواذ على القوة الإلكترونية،ويتم استخدام الفضاء الإلكتروني في الاستعداد لحرب المستقبل والقيام بتدريبات على توجيه ضربة أولى لحواسب العدو، واختراق العمليات العسكرية عالية التقنية، أو حتى باستهداف الحياة المدنية والبنية التحتية المعلوماتية. ولعل الهدف من وراء ذلك؛ تحقيق "الهيمنة الإلكترونية الواسعة" بشكل أسرع في حالة نشوب صراع.

المطلب الثاني: مخاطر عسكرة الفضاء الالكتروني.

أدت علاقة الفضاء الإلكتروني بعمل المنشآت الحيوية سواء أكانت مدنية أو عسكرية لقابلية تعرضها لهجوم من خلاله إما يستهدفه كوسيط وحامل للخدمات أو بشل عمل أنظمتها المعلوماتية، ويكون من شأنه التأثير على القيام بوظيفتها ومن ثم فإنّ التحكم في تنفيذ هذا الهجوم يعد أداة سيطرة ونفوذ استراتيجية بالغة الأهمية سواء في زمن السلم أو الحرب.[1]

أصبح للفضاء الإلكتروني دور فيما يطلق عليه "القوة المؤسسية"في السياسة الدولية والتي تعني أن يكون لها دور في قوة الفاعلين وتحقيق أهدافهم وقيمهم في ظل التنافس مع الآخرين، والمساهمة في تشكل الفعل الاجتماعي في ظل المعرفة والمحددات المتاحة والتي تؤثر في نظريات العلاقات الدولية وتشكيل السياسة العالمية.[2]

وأثّر المجال الالكتروني في تشكيل قدرة الأطراف المؤثرة، والتي يعد من أبرزها الأطراف الدولية الناشئة، مثل الولايات المتحدة التي كان لديها ما يشبه الاحتكار لمصادر القوة منذ نهاية الحرب الباردة،ولتظهر عملية انتقال القوة وانتشارها بين أطراف متعددة سواء أكانت دولاً أو من غير الدول.[3]

وشهد المجتمع الدولي اتجاهات التحول في قضية التعامل مع تهديدات الفضاء الالكتروني وإمكانية تحول الفضاء الالكتروني نحو العسكرة وبرز ذلك في عدة اتجاهات لعل أهمها، تصاعد الهجمات الالكترونية

---

[1]– عادل عبد الصادق، **الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق**، (القاهرة: المكتبة الأكاديمية، 2016): 22-265.

[2]- David Held *et al.*,*Global Transformations: Politics, Economics, and Culture* (California: Stanford University Press, 1999).

[3]- Joseph S. Nye.*The Future of Power* (New York: Public Affairs, 2011).

ومخاطرها على أمن الفضاء الالكتروني، والتطور في مجال سياسات الدفاع والأمن الالكتروني، وتصاعد القدرات في سباق التسلح السيبراني عبر الفضاء الإلكتروني وتبني سياسات دفاعية سيبرانية لدي الأجهزة المعنية بالدفاع والأمن، وتصاعد حجم الإستثمار في مجال تطوير أدوات الحرب السيبرانية داخل الجيوش الحديثة.[1]

[1]– عادل عبد الصادق، **الحروب السيبرانية؛ تصاعد القدرات والتحديات للأمن العالمي**، مرجع سابق.

المبحث الثالث: نظريات وأبعاد ومداخل الأمن السيبراني.

المطلب الأوّل: نظريات الأمن ومستوياته.

أوّلا: نظريات الأمن.

وضع الإنسان، نصب عينيه، فكرة مثالية عن أمنه الذاتي، متخيلاً ما يصبو إليه من مأكل ومشرب وملبس، وأسرة ومسكن، ودخل ينفق منه، ويشتري به كل مستلزماته، الضروري منها والكماليّ.

وانتقلت فكرة الأمن المثالي هذه، إلى المجتمعات والدول، التي كونها الإنسان على مر العصور. ولم تكن الفكرة متطابقة في كل المجتمعات، فهي وإن تشابهت في مضمونها، إلاّ أنها اختلفت في طرق تحقيقها. فهناك دول زراعية، وأخرى صناعية، وثالثة تجارية. وكما اختلف مستوى البشر، طبقاً لما قدره الله لهم من رزق، وسعى كل فرد إلى رزقه، فإن الدول كذلك اختلف مستواها، فهناك دولة غنية، وأخرى متوسطة الغنى، وثالثة فقيرة. وسعت كل دولة، من خلال إمكاناتها، إلى تحقيق فكرتها عن الأمن المثالي (الأمن المطلق) Absolute Security.[1]

ساد المجتمع الدولي نظريتان متضادتان، لفكرة تحقيق الأمن المطلق. وكان مقياس تبني الدول لأحد تلك النظريتان، يرجع إلى المكانة الدولية للدولة:

1. نظرية الدولة العالمية للأمن International State Security

مؤيدو هذه النظرية، دائماً من الدول العظمى والكبرى، عالمياً أو إقليمياً، لذلك فإنهم يرون . طبقاً لمفهوم النظرية . "أن الأمن المطلق لا يتحقق إلا في وجود دولة عالمية (أو إقليمية)، تحتكر كل أسباب القوى"، وهو مفهوم الولاية القوية نفسه، في الإمبراطورية قديماً.

النقد الذي وجه إلى هذه النظرية، يوضح أن الدولة العالمية، ما هي إلا مرادف للدولة القومية، ذات الصبغة السياسية الاستعمارية، "فكل ما تضيفه الدولة العالمية لقواها لتحقيق أمنها المطلق، هو انتقاص من أمن الدول

[1]- نظريات الأمن الوطني ومستويات – مقاتل الصحراء، مقال على الموقع الإلكتروني: www.moqatel.com، بتاريخ: 2019/03/18، على الساعة 18:30.

الأخرى، التي أصبحت جميعها معرضة للخطر". أي إن تحقيق الأمن المطلق في هذه النظرية، يعتمد على القوة والإكراه للآخرين.

2. نظرية المجتمع العالمي للأمن Universal Association

معظم الدول تؤيد هذه النظرية، فهي نظرية الأغلبية من الدول غير العظمى أو الكبرى، التي تخشى نفوذ القوى الكبرى والعظمى وهيمنتها، مما سينقص من أمنها بدلاً من بلوغه الكمال والمثالية. وتفرض هذه النظرية، نظرة معاكسة لسابقتها (نظرية الدولة العالمية للأمن)، لذلك فهي تقر "أنّ الأمن لا يحتاج بالضرورة وجود الدولة، وإنما يمكن تحقيق مفهوم جيد للأمن بانضمام الجميع إلى جمعية عالمية، دولاً وأفراد. وأن يكون العمل الجماعي، لصالح الجماعة كلها، هو الدعامة القوية لضمان الأمن". هو ما يعني الاختيار الحر لتطبيقات الأمن، دون إكراه من أحد، وهي النظرة الأقرب للمثالية.

ومن المفارقات أن الدول الكبرى إقليمياً، تعتنق النظرية الأولى على المستوى الإقليمي حيث تحاول أن تفرض نظرتها لمفهوم الأمن على الآخرين داخل الإقليم، بينما تؤيد النظرية الثانية في تعاملاتها الدولية. والملاحظ أن معظم هذه الدول، إما أن تكون تحت حكم الفرد (دكتاتورية مطلقة)، أو أن تكون ذات ميول توسعية عدوانية ومشمولة برعاية عالمية.[1]

ثانيا- مستويات الأمن:

عندما اتضح أن الأمن المطلق المثالي يصعب تحقيقه، وأن تعارض الأهداف والمصالح القومية للدول، توقعها في مصادمات، تكون من نتائجها انتهاك الأمن الوطني للفريق الخاسر، في كل أو بعض مكوناته. وضعف للأمن الوطني للفريق الغالب في بعض الأحوال، سعت الدول إلى علاقات دولية وإقليمية تزيد بها من صلابة أمنها الوطني، وتغطي نقط ضعفه، في إطار المصلحة العامة، وتتلاقى الأهداف دون تعارض، وهو أمر ليس بالسهل كذلك، يسعى لمصلحة مطلقة لتحقيق الأمن الوطني، وهي فكرة قريبة الشبه من الأمن المطلق. بل استطاعت المصلحة العامة المطلقة، أن تجمع بين دول أكثر عدداً، وأكثر اختلافاً في قاعدتها، التي يُطلب

[1]- **جمال منصر، استراتيجية جديدة لاحتواء جهوي شامل،** مذكرة ما جستير، قسم العلوم السياسية، جامعة ، باتنة، 2003، ص 68.

لها الأمن الوطني (خصائص الدولة وشعبها)، سعياً لتحقيق الأمن الوطني لكل منهم، بتحقيق أمن جماعي لهم جميعاً، خوفاً من تكرار تجربة أليمة مضت.

ومن هذا المفهوم، بدأ في الظهور عدة تكتلات، لها عدة أهداف على الصعيد الاقتصادي والاجتماعي والسياسي. وبدخول التعاون العسكري، تكتمل الصفة ليصبح التكتل ذا صبغة أمنية متكاملة. وتكررت ظاهرة مشاركة الدولة في العديد من التنظيمات، سعياً وراء مزيد من الضمان لأمنها الوطني، في بعض، أو كل مقوماته.

وصُنفت تلك التكتلات في مستويات، تتدرج من الفردية (الذاتية)، إلى الدولية (الجماعية)، لإدراك مجالاتها وتحديد اتجاهاتها الأمنية:

1. المستوى الأول، الأمن الداخلي Individual Security

أدنى درجات الأمن، وأساسها أيضاً، وهو يُعني بالحالة التي يوجد عليها الفرد (المواطن)، من استقرار وطمأنينة، وعدم تهديد لوجوده وبقائه، لذلك يعرف أيضاً بمسمى "الأمن الفردي". وهو ذو مظهرين، أحدهما مادي، وهي مجالات الأمن الأساسية لدى الفرد (المواطن) من مورد رزق يوفر ضروريات الحياة، له ولأسرته، من مأكل ومشرب وكساء، ومأوى (سكن) دائم وآمن، والاطمئنان على حياته وأسرته من اعتداء الآخرين. المظهر الثاني معنوي (نفسي)، يحقق الحاجات النفسية للإنسان من الاعتراف بوجوده وفائدته للمجتمع (البيئة)، الذي يعيش فيه، وأهمية نشاطه ودوره للجماعة والمجتمع، ومنحه مركزاً مميزاً في المجتمع تقديراً له.

هذا الشق الأمني (أمن المواطن الداخلي) هو من مسؤوليات الدولة، وشأنها الداخلي مع مواطنيها. ومحصلة تحقيق هذا الأمن لجموع الشعب كأفراد، وجماعات، وطوائف، ومدن وولايات (محافظات . أقاليم . مناطق) هو تحقق للأمن الداخلي، للدولة نفسها.[1]

ومع ذلك، فإن المنظمات العالمية، والمؤسسات غير الحكومية، صاغة هذا الأمن في مواثيقها باسم حقوق المواطنة، أو حقوق الإنسان وغيرها. وهو ما يعكس قلق الدول الأعضاء في تلك المنظمات، أو

[1]- **استراتيجية جديدة لاحتواء جهوي شامل** ، المرجع السابق ص74.

الجماعات المؤسسة لها (في حالة كونها منظمة غير رسمية)، من انتهاك أمن المواطن (الفرد) وانعكاسات ذلك على أمن الدولة أو أمن المجتمع، الذي يمكن أن يستشري، فيصيب ما جاوره من دول ومجتمعات فيهدد أمنها.

2. المستوى الثاني، الأمن الوطني National Security

القصد منه ضمان تأمين الدولة من الداخل، مع توافر القدرة على دفع التهديد الخارجي، وصولاً لتحقيق حياة آمنة مستقرة، في إطار حدود الدولة، والتزاماتها السياسية. وهو مستوى مركب من عدة جزئيات، فالأمن الداخلي لهذا المستوى يسمى الأمن المحلي Local Security، وهو جزء من البعد السياسي للأمن. والأمن الذاتي Regime Security جزء من الأمن المحلي، وهو أمن خاص بالنظام الحاكم، الذي يشمل إجراءات المحافظة على الشرعية الدستورية للحكم، أو إجراءات الحفاظ على الوضع القائم، وبقاء النخبة الحاكمة في السلطة.[1]

ويطلق على هذا المستوى أحياناً "الأمن القومي"، وهي تسمية مرادفة، دون أن يكون لها صفة قومية، كما يدل الاسم في بعض الدول. كما تعني في دول أخرى تجمع قومية بعينها. وهذا التفسير لمعنى "الأمن القومي"، يتداخل مع مستويات أخرى تالية.

ويعتبر الأمن الوطني، المستوى الأساسي للأمن، والذي تسعى الدول لتحقيقه، داخلياً وخارجياً. وتنهج كل السبل الممكنة في سبيل ذلك، بما فيها الصراع المسلح للدفاع عنه.

3. المستوى الثالث، الأمن دون الإقليمي Sub-Regional Security

يُعني هذا المستوى، بتأمين متطلبات الأمن، لعدد محدد من الدول، في إطار مصلحة مشتركة، سواء كان ذلك من خلال ترتيبات أمنية فقط، أو تنظيم كامل (منظمة). وتكون هذه الدول غالباً عضو في تنظيم أوسع، يتيح لها الاشتراك في منظمة (دون الإقليمية)، والتركيز على مصلحة مشتركة تجمع هذه الدول في التنظيم دون الإقليمي. مثال ذلك مجلس التعاون لدول الخليج العربية، ومجلس التعاون العربي، والاتحاد المغاربي، وكلها نشأت في توقيتات متقاربة، لأسباب مختلفة. فالأول أنشئ عقب اندلاع حرب الخليج الأولى بين العراق وإيران، لمواجهة أخطار هذه الحرب (العسكرية، والاقتصادية، والسياسية)، وتحقيق المصلحة المشتركة بين

[1]- نظريات الأمن الوطني ومستويات، مرجع سابق.

أعضاء هذه المنظمة، بسبب تخوفهم من تأثير الحرب على البعد الاقتصادي للأمن، خاصة إذا أثرت الحرب على صادرات النفط وأسعاره. ويجمع بين دوله، أيضاً، الأصول العرقية، واللغة، والدين، والتاريخ المشترك، وجميع دوله عضوٌ في تنظيم أوسع، (جامعة الدول العربية)، ذي صبغة قومية عربية فقط. أما الثاني فقد أنشئ لهدف اقتصادي في البداية، وهو تنمية اقتصاد دوله الأعضاء، وعندما اختلفت وجهات النظر الأمنية للأعضاء (خاصة بعد غزو العراق للكويت)، لم يكن من الممكن استمراره، فتم حله. ومثل سابقه، فدوله جميعها أعضاء في تنظيم أوسع (جامعة الدول العربية). والثالث هو اتحاد دول المغرب العربي، وهو تجمع كان الهدف منه اقتصادي وسياسي، ولكن فاعليته ضعيفة، حيث لا يوجد له إطار أمني حتى الآن، على الرغم من أن هدفيه هما أهم أبعاد الأمن الوطني. وقد يكون ذلك للمتناقضات التي تحتويها دوله الأعضاء. ومن المفارقات أن هذا التنظيم هو الوحيد . وقد يكون ذلك على مستوى العالم أيضاً . الذي تشارك دوله جميعاً في عضوية عدة تنظيمات أوسع (جامعة الدول العربية، ومنظمة الوحدة الأفريقية)، وكل منهما له صبغة مختلفة تجتمع في دول الاتحاد.[1]

ويرى بعض الدارسين، أن المنظمات دون الإقليمية، المتفرعة من تنظيم إقليمي أوسع (كما في حالة المنظمات الثلاث السابقة ومنظمة جامعة الدول العربية)، أنها تتيح خصوصية زائدة لأعضاء التنظيم دون الإقليمي، بما يفترض معه رؤى أمنية خاصة يحققها هذا التجمع (أمن الخليج والنفط، في حالة مجلس التعاون الخليجي)، والذي يُفضّل معه عدم إشراك التجمع الأكبر، من دون أن يتعارض ذلك مع أمن التجمع الأكبر، من منظور أن تحقيق الأمن للمستوى الأقل، يعاون على تحقيق الأمن للمستوى الأكبر.

4. المستوى الرابع، الأمن الإقليمي Regional Security

ظهر مصطلح "الأمن الإقليمي"، في الفترة التي أعقبت الحرب العالمية الأولى، ليعبر عن سياسة تنتهجها مجموعة من الدول، تنتمي إلى إقليم واحد، وتسعى للتنسيق الكامل لكافة قدراتها وقواها لتحقيق استقرار لأمنها في محيط الإقليم، بما يردع التدخلات الأجنبية من خارج الإقليم، والدول المجاورة المهددة له. وقد انتشر استخدام هذا المصطلح عقب الحرب العالمية الثانية، بظهور تنظيم إقليمي اهتمت معظم دول العالم به، وهو جامعة الدول العربية. وقد أنشأتها الدول العربية عام 1945، اعتماداً على القومية العربية، التي تجمع

---

[1]- نظريات الأمن الوطني ومستويات، مرجع سابق.

شعوب هذا التنظيم. إضافة إلى تجاورها في المنطقة العربية لتجمع هذه الدول بين الأصل العرقي الواحد، والتشابه السكاني (دين ولغة وتقاليد) والانتماء الإقليمي الواحد، وهو ما لم يتجمع في أي تنظيم آخر.

5ـ المستوى الخامس، الأمن الدولي Universal Security

قرب انتهاء الحرب العالمية الثانية، بحثت الدول الكبرى المنتصرة (الولايات المتحدة الأمريكية، والاتحاد السوفيتي، والمملكة المتحدة)، وضع صيغة أمنية عالمية. وإقامة تنظيم دولي جديد، يستند إلى مبادئ وأسس دولية، بعد ما تبين عدم فاعلية الهيئة السابقة (عصبة الأمم)، التي أنشأت عقب الحرب العالمية الأولى، ولم تستطع منع نشوب حرب عالمية أخرى، لعدم مواءمة أجهزتها وميثاقها لمتغيرات المجتمع الدولي. صدر في 7 أكتوبر 1944 مقترحات للأسس والمبادئ، التي سينشأ عليها التنظيم الدولي الرسمي الجديد، تحت اسم "هيئة الأمم المتحدة".

المطلب الثاني: أبعاد الأمن السيبراني.

يطاول الأمن السيبراني جميع المسائل الاقتصادية، والإجتماعية والسياسية، والإنسانية، وذلك انطلاقا، من التعريف المعطى له، على أنّه قدرة الدولة على حماية مصالحها وشعبها، في مختلف مجالات حياته اليومية، ومسيرته نحو التقدم، بأمان، من جهة أولى، ومن كونه يرتبط ارتباطا وثيقا بسلامة مصادر الثروة في العصر الحالي، ونعني بها، البيانات، والمعلومات، والقدرة على الاتصال والتواصل، وهي المحور الذي يتكون حوله الإنتاج، الإبداع والقدرة على المنافسة، من جهة ثانية.[1]

من هنا لا بد من التوقف عند أبعاد الأمن السيبراني، على أن نستعرضها كما يلي:

أوّلا- الأبعاد العسكرية.

من المعلوم، أنّ بدايات الانترنت، قد طورت في بيئة عسكرية، بشكل أساسي، لتضاف إليها فيما بعد البيئة الأكاديمية، بما تمثل من أبحاث تخدم تطوير القدرات العسكرية، والانجازات العلمية، التي تحافظ على تفوق بلد على آخر، حيث كان التنافس على أشده، بين الاتحاد السوفياتي، والولايات المتحدة الأميركية، في

---

[1]- منى الأشقر جبور، **الأمن السيبراني: التحديات ومستلزمات المواجهة**، (بيروت: الملتقى السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، 27-28 أغسطس 2012)، ص 14.

مجال الوصول إلى الفضاء الخارجي، وتطوير الأسلحة النووية. وتتراكم الأمثلة التي يمكن سوقها، في هذا المجال، لتوضيح الأبعاد العسكرية، للأمن السيبراني، وخطورة الهجمات السيبرانية، حيث يمكن إيراد ما حصل في جورجيا، واستونيا، وكوريا الجنوبية، وإيران، كمثال على بعض الهجمات والاختراقات، التي ترجمت ماديا، سواء باندلاع صراع مسلح لاحق، كذلك الذي وقع، بين روسيا وجورجيا، أو بانقطاع الاتصال بالانترنت في استونيا، بين الدولة والمواطنين، والتشويش على الإدارات الحكومية.

كذلك، ترد هنا، اختراقات أنظمة المنشآت النووية، في إيران، وتحقق إمكانات التلاعب بها، مع ما يعنيه هذا من تعرض الأمن القومي، للدولة المعنية، ومن تعريض السلام الدولي للاهتزاز. في هذا المجال أيضا يمكن إيراد، الاختراق الذي حصل في البرازيل، والمملكة المتحدة، للبنية التحتية للطاقة، حيث انقطع التيار الكهربائي، ما طال بآثاره السلبية ملايين الأشخاص، والمؤسسات والمصالح، وما يمكن أن يعني من وصول إلى موارد الطاقة كافة.[1]

ثانيا- الأبعاد الاجتماعية.

تسمح طبيعة الانترنت المفتوحة، عبر المدونات والشبكات الاجتماعية بشكل خاص، لكل مواطن، بان يعبر عن تطلعاته السياسية، وطموحاته الاجتماعية، بأشكالها كافة. كذلك، تشكل مشاركة جميع شرائح المجتمع ومكوناته، وسيلة لإغناء هذا المجتمع، وتطويره، بما تتيحه من فرص للاطلاع على الأفكار، والمعلومات، المختلفة، وبما تكونه من حاجة لدى الجميع، في الحفاظ على استقرار الفضاء السيبراني، والمجتمع الذي يرتكز إليه. والمعلوم أنّ انفتاح مجتمع ما، على مجتمع آخر، يؤسس لتبادل خبرات، وأفكار، وتكون حاجات جديدة، وآفاق تعاون وتكامل.

يضاف إلى هذا ما تقدمه الانترنت من إمكانات وقدرات، للمجالات العلمية، والثقافية، والخدماتية، حيث تسمح بالوصول إلى مناطق بعيدة، والى فئات محددة، ككبار السن، والمرضى، وغيرهم من ذوي الاحتياجات الخاصة. هذا عدا عن الدور، الذي يمكن ان تؤديه، في تبادل المعلومات، في أوقات الأزمات الإنسانية والكوارث، بحيث تتأمن المساعدات وتوزع بالسرعة المطلوبة. ولا تقف الأبعاد الاجتماعية، عند حدود توفير اطمئنان المواطن إلى حياته اليومية، والإفادة من طاقات تقنيات المعلومات والاتصالات، في تطوير

[1]– نفس المرجع، ص 14.

نشاطاته المختلفة، بل تتعداها إلى صيانة القيم الجوهرية في المجتمع: كالانتماء، والمعتقدات، إضافة إلى العادات والتقاليد. في هذا السياق، يأتي التشديد من قبل المنظمات والهيئات الدولية، على نشر ثقافة الأمن في الفضاء السيبراني، وضرورة تعاون المجتمع، بكل مكوناته، على تحقيق الأمن السيبراني وضمانه. فمما لا شك فيه، أنّ المخاطر السيبرانية، تطاول المجتمع ككل، سواء، بسبب ارتكاز الخدمات الحيوية، كالطاقة، والنقل، والصحة، والاتصالات، وغيرها، على ما تقدمه تقنيات الاتصالات والمعلومات، من إمكانات، أو عبر ما يضخ من محتوى في الفضاء السيبراني. فالمحتويات غير المشروعة، وغير المرغوب بها، ذات تأثير سلبي أكيد، على أخلاقيات مجتمع معين، وعلى ارتفاع نسبة الممارسات الإجرامية. أما الأمثلة التي تساق هنا فكثيرة، ونذكر منها: الإباحية، والترويج للاتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام الدوليين. وعليه، لابدّ من بناء مجتمع مسؤول، ومدرك لمخاطر الفضاء السيبراني، قادر على التعامل بحد أدنى من قواعد السلامة، مع إدراك للعواقب القانونية، التي يمكن أن تترتب على التصرفات، والتي تعرض سلامة الغير، وسلامة رؤوس الأموال وحركتها، للخطر.[1]

ثالثا- الأبعاد السياسية.

تتمثل الأبعاد السياسية للأمن السيبراني، بشكل أساسي، في حق الدولة في حماية نظامها السياسي وكيانها، ومصالحها الاقتصادية، التي تعني، حقها وواجبها في السعي إلى تحقيق رفاه شعبها، في وقت تؤثر التقنيات، في موازين القوى داخل المجتمع نفسه، حيث أصبح بإمكان المواطن، أن يتحول إلى لاعب أساسي في اللعبة السياسية. كما أصبح بإمكانه الاطلاع، على خلفيات ومبررات القرارات السياسية، التي تتخذها حكومته، عبر الكم الهائل من المعلومات، التي يمكنه الوصول إليها، أو التي يمكن أن توزع وتنشر على الانترنت، وبقية الأجهزة التي توصل بها. بالمقابل، لا يتوانى العاملون في الشأن السياسي، عن الإفادة مما تقدمه هذه التقنيات، للوصول إلى أكبر شريحة ممكنة من المواطنين، والترويج لسياساتهم، في العالم. وغني عن البيان مدى التأثير الذي يتركه هذا الأمر بغض النظر عن صحة السياسات، والمبادئ والمواقف التي يروج لها.[2]

---

[1]– منى الأشقر جبور، **الأمن السيبراني: التحديات ومستلزمات المواجهة**، مرجع سابق، ص 16.

[2]– نفس المرجع، ص 17.

رابعا- الأبعاد الاقتصادية.

يرتبط الأمن السيبراني ارتباطا وثيقا بالاقتصاد. فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة والمخزنة والمستخدمة على كل المستويات. كذلك تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لبلدان كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية والشركات الكبرى التي تبحث عن إدارة كلفة إنتاجها، بأفضل الشروط. إلاّ أنّ هذا الواقع المشرق، يطرح مسائل مختلفة، سواء منها ما يتعلق بحماية مقدم الخدمة والعمل، أو بحماية المستهلك على الانترنت. يضاف إلى ذلك دخول العالم، عصر المال الالكتروني، ضمن بيئة تقنية متحركة، بعد إطلاق خدمات المحفظة الالكترونية، إذ تتزايد استثمارات المصارف، والمؤسسات المالية، في مجال المال الرقمي. وتتنافس الشركات، على إصدار تطبيقات، تسمح بآليات دفع آمنة وبحفظ المال في المحفظة الالكترونية وبالإيفاء من خلالها، وباستخدامها كرصيد افتراضي، وقد وضعت بعض الدول تشريعات خاصة بهذا المال[1]. وغني عن القول، ما يمكن أن يثيره هذا الأمر، من صعوبات، وما يتطلبه من تشريعات، للحد من بعض الجرائم الاقتصادية والمالية الخطرة، والعابرة للحدود، كتبييض الأموال، والتهرب من الضريبة.

ويربط المسؤولون عن مقدرات الحكومات، وسياساتها، بين الأمن والنمو الاقتصادي، بشكل واضح. فالأمن السيبراني، يضمن ركون الجمهور، إلى الخدمات التي تقدم بواسطة تقنيات المعلومات والاتصالات، كما يضمن الإقبال عليها، بما يترجم عمليا، بتطوير أسس اقتصاد سليم. ولعل الدليل الأوضح، على هذه القيمة، هو استهداف هذه المعلومات، منذ القديم، سواء من خلال عمليات التجسس الصناعي والعسكري التقليدية، أو من خلال الاعتداء على الملكية الفكرية. هذا عدا عن التأثيرات المالية السلبية التي يتركها الاعتداء على أنظمة المعلومات وتعطيلها. إلاّ أنّ الأبعاد الاقتصادية يمكن أن تتجاوز خسائر عدم استخدام تقنيات الاتصالات والمعلومات، إلى خسائر تقدر بمليارات الدولارات[2].

---

[1]- Electronic money regulations 2011 (EMR 2011) & the payment Services Regulations .2009

[2]- Senators Unveil Major Cybersecurity Bill Measure Would Update FISMA, Encourage Sharing of Cyber threats By Eric Chabrow, *February 14, 2012.* "Sen. Susan Collins, R-Maine, one of the bill's sponsors, said in a Senate speech. "The threat is not just to our national security, but also to our economic well-being." http://www.govinfosecurity.com/articles.php?art_id=4506&opg=1

خامسا- الأبعاد القانونية.

يرتب النشاط الفردي والمؤسساتي والحكومي في الفضاء السيبراني نتائج قانونية وموجبات تستدعي اهتماما لجهة إيجاد القواعد الخاصة، بحل النزاعات التي يمكن أن تنشأ عنها. لذا لابدّ من مراعاة بعض التحولات التي رافقت ظهور مجتمع المعلومات. فإلى جانب الحقوق الأساسية والحريات الإنسانية المعترف بها في الدساتير والتشريعات الدولية، أضيفت حقوق أخرى كحق النفاذ إلى الشبكة العالمية للمعلومات، كما توسعت بعض المفاهيم، لتشمل أساليب الممارسة الجديدة باستخدام تقنيات المعلومات والاتصالات، كالحق في إنشاء المدونات الالكترونية والحق في إنشاء التجمعات على الإنترنت، كما الحق في حماية ملكية البرامج المعلوماتية. كذلك برزت موجبات جديدة ذات انعكاسات اقتصادية ومنها على سبيل المثال: موجب الاحتفاظ ببيانات الاتصالات وموجب الإبلاغ عن مخالفات وجرائم خاصة بالمحتوى.

يضاف إلى هذا ما يتوقع من تحولات على مستوى سياسات القطاعات الصناعية والتجارية على ضوء الحاجة إلى إعادة صياغتها، بما ينسجم مع توسع استخدام الشبكات الاجتماعية، والمسائل القانونية التي لا بد وأن تثار، على مستوى حماية المستهلك، والخصوصية، والبيانات الشخصية، وحقوق العمال والمستخدمين، والملكية الفكرية. فالسنوات القادمة. ومما لا شك فيه أنّ النزاعات القانونية ستطال الإعلان الذي يرتكز إلى أطياف مستخدمي الإنترنت انطلاقا من اهتماماتهم البحثية أو المواقع التي يزورونها، والاختراقات، والتسريبات للبيانات الشخصية والمالية سواء منها المقصودة أو غير المقصودة، ومسؤوليات الجهة التي تملكها أو تديرها والحق في تصحيح البيانات الشخصية، ومحوها، وتعديلها.[1]

[1]- منى الأشقر جبور، **الأمن السيبراني: التحديات ومستلزمات المواجهة**، مرجع سابق، ص 18.

الفصل الثاني: الإستراتيجية الروسية للأمن والدفاع في فترة فلاديمير بوتين 2014-2009

تمهيد:

تعتمد جل الدول الى تبني استراتيجية خاصة ،فهناك بعض الدول تتبنى استراتيجية دائمة في حين ان هناك دول اخرى تتبنى استراتيجيية مؤقتة ،كما تختلف كل استراتيجية من فترة الى اخرى و ككل الاستراتيجيات مرت الاستراتيجية الروسية بمراحل مختلفة،خاصة كون روسيا لا تزال تتمتع بثقل سياسي على المشهد الدولي ،حيث تسعي روسيا إلى إعادة دورها العالمي أدّى إلى توسع دوائر الإهتمام وهو ما أخلها في المنافسة مع الدول الأخرى في كثير من القضايا ممّا يجعلها عرضة للكثير من التهديدات الخارجية والداخلية على أمنها.

وهكذا هدفت الاستراتيجية الروسية الى اعطاء اولوية لتطوير دور روسيا في عالم متعدد الاقطاب لا يخضع لهيمنة قوة عظمى واحدة .حيث بدت ملامح الاستراتيجية الروسية اكثر وضوحا و صلابة منذ استلام الرئيس "فلاديمير بوتين" مقاليد الحكم، وظهر ذلك من خلال اعتماد روسيا على قوة عقيدتها العسكرية لتحديد أهدافها الإستراتيجية.

المبحث الأول: الخصائص العامة للإستراتيجية الروسية في عهد فلاديمير بوتين (2009 – 2014).

المطلب الأول: سمات الإستراتيجية الروسية.

تحدّدت سمات الإستراتيجية الروسية بعد انتهاء الحرب الباردة من خلال تحديد أهم معالم توجهات روسيا الاتحادية الإستراتيجية، والتي تتمثل فيما يلي:[1]

1–الواقعية: تتجسد هذه السمة في سعي القيادة السياسية الروسية إلى بناء سياسة براغماتية، عن طريق الابتعاد عن الحجج الأيديولوجية، التي كانت تميز التحرك الدبلوماسي والسياسي السوفياتي في الماضي القريب، وإحلال محلها مبررات سياسية واقتصادية أكثر وضوحا وتعبيرا عن تطلعات روسيا المستقبلية.

2– براغماتية القيادة: وتتمثل في لجوء القيادة الروسية إلى قيم جديدة بدأت تعمل بها، حيث عمد رؤساء روسيا إلى إظهار وتأكيد قطع علاقات بلادهم بالماضي الشيوعي، والتخلي عن كافة ركائز الحرب الباردة، بما فيها الأيديولوجيا الماركسية اللينينية.

3– الديناميكية: وتظهر ديناميكية أو فاعلية الإستراتيجية الروسية من خلال ما يضمن بصورة جدية عدم العودة إلى الوراء منذ تواري عصر الأيديولوجيات المتصارعة على الساحة الدولية أو غياب الأيديولوجيا الشيوعية، حيث ظهر فلاديمير بوتين في نظر الغرب كحام للخط الإستراتيجي الجديد الذي انتهجته روسيا في عصر العولمة وحرية الأسواق، مع الإصرار على وحدة تراب الاتحاد الروسي وعدم التفريط بها، واتباع مختلف الوسائل، بما فيها القوة العسكرية، لتأكيد هذه الوحدة، كما في الموقف من تمرد الشيشان.

"أهم هدف تسعى إليه روسيا الاتحادية هو إعادة هيبتها والحفاظ على أمنها وسيادتها من أي خطر يحيط بها، وهو أمر يدفعها إلى تعزيز وضعها العسكري في المناطق الحدودية".[2]

---

[1]– الإستراتيجية الروسية بعد الحرب الباردة، موقع إلكتروني: https://www.aljazeera.net/knowledgegate/books، بتاريخ: 2019/04/12، على الساعة: 16:09.

[2]– نفس المرجع.

4– المنافسة: وهي هدف جديد على السياسة الروسية، ولأجله أجاز الدستور الروسي الجديد هدف المنافسة على الأسواق العالمية محل المواجهة الأيديولوجية. لكن تحقيق هذا الهدف لا يخلو من الصعوبات، التي سرعان ما انعكست على الإستراتيجية الروسية، من خلال إعادة ترتيب الأولويات، الذي انعكس في خطط الإصلاحات البنيوية الجديدة، وحركة الانفتاح المالي والاقتصادي على الخارج.

وهذا يظهر الفارق بين الإستراتيجية الروسية الحالية وما كان متبعا في الحقبة السوفياتية، إذ خلافا للاتحاد السوفياتي، تفضل روسيا الاتحادية، ولأسباب اقتصادية بالدرجة الأولى، إرسال المزيد من الأسلحة إلى الدول التي تستطيع دفع ثمنها. وتؤكد المؤلفة أن بلوغ هذه الغاية يتطلب المزيد من الاستثمارات من جهة، والإصلاح البنيوي للقاعدة الصناعية الروسية لرفع مستواها التنافسي من جهة أخرى.

5– حرية الحركة: وتتجسد في أن تفكك الاتحاد السوفياتي وظهور نظام دولي جديد لم يصاحبهما فرض شروط على روسيا أو على مصالحها أو على حرية حركتها أو عناصر قوتها، فوضعها الجديد لم يجعلها، على الأقل، مجبرة على الانصياع لموقف الدول الكبرى، سواء داخل مجلس الأمن ضمن منظمة الأمم المتحدة، أو خارجه ضمن توجهات التطام الدولي الجديد، الأمر الذي مكنها من القدرة على التحرك والتحدي والمعارضة لأي نمط جديد في العلاقات الدولية، وبما يتفق مع مصالحها.

6– المرونة: وتظهر من ملاحظة الاختلاف في المفاهيم بين الولايات المتحدة الأميركية وروسيا الاتحادية بخصوص مسألة الأمن العالمي وموقع المصالح الروسية منها. ففي حين ترى الولايات المتحدة مناطق العالم الحساسة على أنها جزء من النفوذ الغربي، وعلى الغرب تأمين الحماية اللازمة للمحافظة على الوضع السياسي القائم فيها، تؤيد روسيا الجهود الجماعية، والاقتراح الداعي إلى إشراك جميع أعضاء مجلس الأمن والأطراف المعنية لحل أي أزمة تنشب في العالم.

لذلك تعتبر روسيا أنّ قضية انضمام جورجيا وأوكرانيا، وحتى أذربيجان، إلى حلف شمال الأطلسي، تشكل خطرا كبيرا على أمنها القومي واستقرارها وإمكانية حركتها وتوجهاتها، سواء على المحيط القريب منها، دول الاتحاد السوفياتي السابق، أو على المحيط الأبعد، مثل الصين أو إيران أو غيرهما من الدول.

ويضاف إليها مسألة نشر الدرع الصاروخية الأميركية في بعض دول الاتحاد السوفياتي (سابقا)، وتجاهل كل الدعوات الروسية لحل هذه المسألة بطريقة تزيل الشكوك الروسية من أنها هي المستهدفة من هذا المشروع.

المطلب الثاني: المحدّدات الرئيسية المتوافرة في الإستراتيجية الروسية.

بعد تولي بوتين السلطة في أبريل 2000، اعتمد إستراتيجية تهدف لدعم سلطة الدولة المركزية، وتشديد قبضتها على المؤسسات الاقتصادية والسياسية وتقوية قدراتها إستراتيجية. وبالتالي بدأ في تقويض سلطة أباطرة رأس المال والسياسة في روسيا واعتقال بعضهم، كما اتجه إلى تعيين حكام الأقاليم الروسية بدلاً من انتخابهم، واختيارهم ممن يعرفهم ويثق في قدراتهم.

وقد أحكم بوتين كذلك سيطرته على ثروات روسيا من النفط والغاز اللذين، حيث تزامن هذا مع ارتفاع أسعارهما في السوق العالمي، ما أدى إلى انتعاش الاقتصاد الروسي، وارتفاع مستوى معيشة الفرد في الدولة الروسية، الأمر الذي زاد من شعبية بوتين داخليا بشكل غير مسبوق.

انعكس هذا بوضوح على سياسة روسيا الخارجية حينما أعلن رئيسها أن سنوات الضعف والمهانة قد ولّت، وطالب الولايات المتحدة وأوروبا بمعاملة روسيا باحترام، وكقوة لها مكانتها ودورها العالمي. واتجه بوتين إلى بناء علاقات شراكة مع كلٍّ من الصين والهند، وإلى استثمار ميراث الاتحاد السوفياتي السابق، وما بناه في مناطق مثل الشرق الأوسط وأمريكا اللاتينية.[1]

تتمثل أهم أهداف السياسة الخارجية الروسية في إضفاء الطابع القومي، وضرورة استرداد روسيا المكانة التي افتقدتها، وإنهاء الانفراد الأمريكي بموقع القمة.

أولاً: أهداف السياسة الخارجية الروسية

الواضح أن بوتين قد كرَّس قدراً ملحوظًا من اهتمامه لصياغة اتجاه جديد وقوي للسياسة الخارجية الروسية، تحاول استعادة المكانة التي كان يتبوأها الاتحاد السوفياتي السابق في مرحلة الحرب الباردة، مع إحداث بعض التغييرات الجوهرية بحيث تتفق مع الوضع الجديد؛ ليمكّنها من تحقيق طموحاتها في عصر العولمة وحرية الأسواق. ولهذا فقد اعتمدت روسيا الاتحادية في سياستها الخارجية عدة دوائر تعتمد على مراحل نموها ومدى استقرارها السياسي والاقتصادي. وفي كل هذه الدوائر كان الهدف الأسمى هو تحقيق الإستراتيجية الأمنية على المدى البعيد.

---

[1]- نبية الأصفهاني: **مستقبل التعاون الروسي- الإيراني في ضوء التقارب الأخير**، السياسة الدولية، العدد 144، المجلد 36، (القاهرة: مركز الدراسات السياسية والإستراتيجية، أبريل 2001)، ص 164.

ويمكن القول إن أهم أهداف السياسة الخارجية الروسية في هذه المرحلة تتمثل فيما يلي:

1- إضفاء الطابع القومي على السياسة الخارجية الروسية، والتأكيد على ضرورة استرداد روسيا المكانة التي افتقدتها منذ قيامها، وإنهاء الانفراد الأمريكي بموقع القمة. وحسب رؤية القيادة الروسية، فيجب إتباع خطة إستراتيجية وعقلانية تفضي إلى إحلال التعددية القطبية محل هذا الانفراد، وعلى نحو يتناسب أكثر واتجاهات العالم الجديد.

2- السعي إلى علاقات متميزة وتعاون إستراتيجي مع أصدقاء الاتحاد السوفياتي السابقين، لاسيما الهند وإيران والصين.

3- الاتفاق مع دول الجوار الإقليمي حول كيفية إقرار السلام والاستقرار في المنطقة.

4- الواقعية في التفكير، وزيادة التعاون وتعزيز العلاقات مع كومنولث الدول المستقلة.[1]

5- السعي إلى تعزيز النفوذ الروسي في الفضاء السياسي للاتحاد السوفياتي السابق.

6- منع انتشار الصراعات السياسية والعسكرية المؤدية لعدم الاستقرار بآسيا الوسطى.

7- تعزيز الديمقراطية في روسيا[2].

وكان من أهم الخطوات التي اتخذها لتقوية سياسة بلاده الخارجية في مواجهة القوى العالمية الكبرى الأخرى اندماج روسيا في العديد من نشاطات السياسة الخارجية مثل مجموعة الدول الصناعية الثماني الكبرى، ومنتدى آسيا- باسيفيك للتعاون الاقتصادي، ورابطة الأمم لجنوب شرق آسيا، ومؤتمرات القمة الروسية مع الاتحاد الأوروبي... إلخ.

[1]- عبد العزيز مهدي الراوي، "**توجهات السياسة الخارجية الروسية في مرحلة ما بعد الحرب الباردة**"، دراسات دولية، العدد 35، ص ص 162- 163.

[2]- نفس المرجع، ص ص 162- 163.

ثانيًا: ملامح تحركات السياسة الخارجية الروسية.

قبل وصول بوتين مرة أخرى إلى سدة الحكم، لوَّح بخطوات قوية لسياسة روسيا الخارجية تنوي بلاده اتخاذها ضد "الشركاء الغربيين" بسبب ما يقومون به مما أسماه "الخطوات الانفرادية على الساحة العالمية، والتي لا تراعي رأي روسيا ومصالحها".

وأكد الرئيس الروسي أنه لا يجوز تحديد قواعد اللعب في الاقتصاد والسياسة الدولية من وراء ظهر روسيا، أو بمعزل عنها وعن مصالحها، مشيراً إلى أن التعاون الدولي طريق ذو اتجاهين، ومشددًا على السعي إلى التعاون البنَّاء والحوار في شأن قضايا مكافحة الإرهاب الدولي، والرقابة على الأسلحة، وصون الأمن العام. وألمح إلى أن الخطوات الانفرادية المشار إليها سلفًا سوف تلقى التقويم المناسب والرد المقابل.[1]

وأشار إلى أن روسيا استعادت خلال السنوات الأخيرة موقعها بين القوى العالمية الرئيسة، معتبراً أن مكانتها الحالية وقدراتها تؤهلها للعب دور أوسع، وتجعل مشاركتها في الشئون الدولية ضرورية أكثر فأكثر.

وفي خضم حملته الشديدة اللهجة على الغرب قبل وعقب انتخابه رئيسًا لروسيا لفترة جديدة، حدَّد بوتين أولويات عمله كرئيس للدولة، مؤكدًا أن إعادة تسليح روسيا أصبحت ضرورية لمواجهة سياسة الولايات المتحدة وحلف شمال الأطلسي في مجال الدفاع الصاروخي، مما يفرض عدم تخلي الدولة الروسية عن قدراتها للردع الإستراتيجي، التي اعتبرها مُشكّلةً للضمانة الأساسية لبلاده، في إشارة إلى السلاح النووي، والصواريخ العابرة للقارات، والمقاتلات، والغواصات، وذلك من خلال أضخم برنامج للتسليح في روسيا منذ استقلاها عام 1991.[2]

---

[1]- عبد العزيز مهدي الراوي، "**توجهات السياسة الخارجية الروسية في مرحلة ما بعد الحرب الباردة**"، دراسات دولية، العدد 35، ص ص 162- 163.

[2]- أحمد دياب، "**عودة بوتين: تحديات وطموحات روسيا بعد انتخابات الرئاسة**"، (القاهرة: السياسة الدولية، العدد 188، مركز الدراسات السياسية والإستراتيجية، أبريل 2012)، ص 106.

وفي هذا الإطار، فقد عارض الرئيس الروسي سياسات الولايات المتحدة والغرب في مد مظلة حلف الناتو إلى الحدود الروسية، ورفض بشدة –ولا يزال– المشروع الأمريكي لبناء قواعد صواريخ مضادة في بولندا وجمهورية التشيك، مستخدمًا لغة قوية في رفض الهيمنة الأمريكية.[1]

المطلب الثالث: القدرات السيبرانية الروسية.

يختلف المنظور الروسي للحرب السيبرانية بشكل واضح عن نظرائه الغربيين، ويبدو ذلك واضحاً في الطريقة التي يعرّف بها المنظرون الروس الحرب السيبرانية؛ والتي تشير إلى كيفية استخدام الكرملين لقدراته على الإنترنت لتحقيق الأهداف القومية لروسيا الاتحادية. فالمسؤولون الروس مقتنعون بأن موسكو تخوض عملية صراع وجودي مستمر مع قوى داخلية وخارجية تسعى إلى تحدي أمنها في عالم المعلومات، ويرون في الإنترنت والتدفق الحر للمعلومات التي يولّدها أنها تشكّل تهديداً وفرصاً يمكن استغلالها بصورة ايجابية لخدمة أهدافها القومية على حدٍ سواء، كما انهم يصورون العمليات الإلكترونية ضمن الإطار الأوسع لحرب المعلومات، والذي هو عبارة عن مفهوم شامل يتضمن عمليات شبكة الحاسوب والحرب الإلكترونية والعمليات النفسية وعمليات المعلومات، وتماشياً مع المفاهيم السوفيتية التقليدية لمحاربة التهديدات المستمرة من الخارج وداخلها، ترى موسكو الصراع داخل "مجال المعلومات" مستمراً ولا يقف عند حدود معينة، بالتالي فإن للكرملين عقيدة معينة في استخدام الإنترنت تختلف عن تلك المتبعة في الولايات المتحدة والدول الأوروبية، كونها تمتاز بطبيعتها الهجومية وسياقها التصعيدي[2].

لقد أنشأت روسيا الاتحادية (وكالة أبحاث الانترنت)، أو ما يُعرف باسم "جيش المتصيدين Troll–Army"، تابع لوكالة الامن الاتحادي الروسي، يضم آلاف الموظفين، ويخصص له سنوياً نحو(300) مليون دولار من ميزانية الدفاع الروسية، إذ يعد الجيش الالكتروني الروسي خامس اقوى جيوش العالم الالكترونية بعد كل من: الولايات المتحدة والصين وبريطانيا وكوريا الشمالية على التوالي، وتتلخص مهمات الجيش الالكتروني الروسي بالآتي:

[1]– أحمد دياب، مرجع سبق ذكره، ص 107.

[2]– أحمد يوسفي الجميلي: **<u>الشؤون العسكرية والأمنية</u>**، (مركز صنع السياسات للدراسات الدولية والأمنية، العدد الأول، 2018)، ص 02، تاريخ الإطلاع: 2019/04/06، على الساعة: 22:01.

•القيام بعمليات التجسس على الخصوم.

•شن الهجمات الالكترونية التي تسبب الضرر للبنى التحتية والاقتصاد والمواقع الحكومية في الدول الاجنبية المعادية .

•حروب المعلوماتية في وسائل الإعلام والشبكات الاجتماعية، عن طريق القيام بعمليات اختراق الحسابات والبريد الالكتروني، وانشاء حسابات وهمية على شبكة المعلومات الدولية، وفتح الآلاف من الحسابات المزيفة على مواقع التواصل الاجتماعي: (تويتر، وفيسبوك،...وغيرها)، للرد على الآلاف من التعليقات والمقالات، ونشر الشائعات وتظليل الحقائق في محاولة لدعم الموقف الروسي وتوجيه الرأي العام ضد الخصوم.

وقد استخدمت روسيا الهجمات السيبرانية بحروبها المختلفة في جورجيا وأوكرانيا وسوريا، إذ يبدو أن روسيا تستخدم الإنترنت كسلاح في العمليات العسكرية التقليدية، حيث أتاحت تجربتها مع كل من جورجيا وأوكرانيا فرصاً لتحسين تقنياتها وإجراءاتها في مجال الحرب السيبرانية وعمليات الارهاب السيبراني، واستعراض قدراتها على الساحة العالمية وشكلت هذه القدرات في عدة مناسبات قوة ردع مهمة ضد خصوم روسيا[1] .

---

[1]– أحمد يوسفي الجميلي، نفس المرجع، ص 04.

المبحث الثاني: عقيدة الأمن السيبراني.

المطلب الأوّل: مفهوم العقيدة الروسية التي أقرّها فلاديمير بوتين.

من منظور ما خلصت إليه الوثيقة الصادرة في 5 فبراير (شباط) 2010 حول العقيدة العسكرية الروسية التي تنص على «إمكانية إعادة النظر في أحكام العقيدة العسكرية بالتغيير والتعديل والإضافة بما يتناسب مع الأخطار والتهديدات لأمن ودفاع البلاد وظروف تطور الدولة الروسية الاتحادية»، عادت موسكو لتطرح ما تراه مناسبا وما يتفق مع الأخطار التي صارت تهدد أمن الدولة في أعقاب اندلاع الأزمة الأوكرانية وما أعلنه حلف الناتو من خطط لتعزيز قواته وقواعده على مقربة مباشرة من الحدود الروسية، فضلا عما عاشته موسكو من مخاوف من احتمالات تأثير أحداث الربيع العربي على الداخل الروسي، وهو ما أفصح عنه صراحة الرئيس السابق ديمتري ميدفيديف.

ويتوقف المراقبون عند ما تنص عليه «وثيقة العقيدة العسكرية الروسية» حول أن «العدو الأول الخارجي لروسيا هو توسع حلف شمال الأطلسي شرقا باتجاه الحدود الروسية»، واعتبارها أن «خطة الولايات المتحدة حول نشر الدرع الصاروخية في أوروبا على مقربة من الحدود الروسية مصدر قلق للأمن القومي الروسي، فضلا عن الأخطار الداخلية، ومنها محاولات تغيير النظام الدستوري والتطاول على وحدة أراضي الدولة من خلال الحركات الانفصالية والإرهاب بكل أشكاله» ما سبق أن عانت منه روسيا في تسعينات القرن الماضي في منطقة شمال القوقاز، وهو ما عكسته وثيقة العقيدة العسكرية الصادرة في 2010.[1]

وقد تناول الرئيس فلاديمير بوتين هذه الموضوعات في اجتماعه الذي عقده في 10 سبتمبر (أيلول) 2014 لبحث المسائل المتعلقة بتحديث منظومة تسليح القوات المسلحة للفترة من 2016 – 2025. وقال بوتين إن الأزمة الأوكرانية تضع الولايات المتحدة نفسها في صدارة قائمة الأخطار المباشرة التي تهدد أمن بلاده، مما يدعو إلى إعادة النظر في العقيدة العسكرية الروسية التي كان أقرها الرئيس السابق ديمتري ميدفيديف في 5 فبراير 2010، وهو ما يعمل الكرملين عليه من أجل إدخال ما يراه مناسبا من إضافات وتعديلات على النص الحالي لهذه العقيدة العسكرية مع نهاية هذا العام بدلا من الموعد المقرر السابق في عام 2020.

[1]– مقال بعنوان: **بوتين.. وعقيدة روسيا الجديدة توسع الناتو والربيع العربي والأزمة الأوكرانية في مقدمة أسباب التفكير في استراتيجيات جديدة**، (الشرق الأوسط: جريدة العرب الدولية، 2014)، ص 01، على الرابط الموالي:
https://aawsat.com/home/article/187566

وتقول معطيات الساحة السياسية المحلية والدولية إن ما يتخذه الرئيس بوتين من قرارات وخطوات، هو رد فعل طبيعي على ما أقرته واشنطن وحلفاؤها من بلدان الاتحاد الأوروبي من عقوبات اقتصادية في إجراء عقابي لما وصفته بأنه تدخل روسيا في الأزمة الأوكرانية. وكان بوتين اضطر إلى اتخاذ بعض الإجراءات الجوابية، ومنها حظر صادرات هذه البلدان من المنتجات الزراعية والغذائية إلى روسيا. ولم يتوقف الرئيس الروسي عند هذا الحد؛ حيث سرعان ما كشف أيضا عن أن بلاده صارت مدعوة إلى تغيير عقيدتها العسكرية، ولا سيما بعد إصرار الولايات المتحدة على نشر عناصر درعها الصاروخية في أوروبا وألاسكا، وتعزيز قوات «الناتو» ونشر قواعد عسكرية جديدة في بلدان شرق أوروبا، على مقربة مباشرة من الحدود الروسية، إلى جانب الاستمرار في خطط عسكرة الفضاء الكوني، ومحاولات استخدام الأسلحة الاستراتيجية بوصفها أسلحة غير نووية. واتهم بوتين الولايات المتحدة بالاستمرار في محاولات استغلال الأزمة الأوكرانية لخدمة مآربها العسكرية الذاتية وإحياء حلف الناتو.[1]

ولعله من مفارقات القدر والموقف، أن يتخذ الرئيس بوتين مثل هذا الموقف مما يؤكد تميزه عن نظيريه السابقين في الكرملين وهما الرئيس الأسبق بوريس يلتسن الذي كان أقر أول عقيدة عسكرية روسية في عام 1993 بموجب نظرية الأمن القومي في ذلك الحين، والرئيس السابق ديمتري ميدفيديف الذي أعلن عن تغيير المذهب العسكري الروسي في صياغة جديدة صدرت في فبراير 2010 على ضوء متغيرات العصر وفي أعقاب حربه التي خاضها ضد العدوان الجورجي ضد أوسيتيا الجنوبية في أغسطس (آب) 2008.

وقد دفعت التطورات الأخيرة في المناطق المتاخمة للحدود الجنوبية لروسيا المسؤولين في وزارة الدفاع الروسية إلى إدراج أخطار أخرى تهدد أمن الدولة الروسية؛ ومنها وجود تنظيم «داعش»، وما أعلن عنه من تهديدات بنقل نشاطه إلى جنوب روسيا والقوقاز، فضلا عن الأخطار الداخلية الناجمة عن محاولات تأليب منظمات المجتمع المدني وازدياد تمويلها من الخارج.

وكان بوتين أعلن في عام 2011 عن تحديث الجيش والأسطول من خلال برنامج طموح حتى عام 2020 تبلغ تكلفته ما يقرب من 500 مليار دولار، قبل أن يعود أخيرا إلى الإعلان عن برنامج تحديث القوات المسلحة للفترة من 2016 – 2025. ورغم حرص بوتين على الإعلان عن أن هذه الخطوات ليست

[1]– نفس المرجع، ص 02.

انجرارا إلى ما يسمونه «سباق التسلح»، وأن موسكو لن تمضي في هذا الطريق إلا بالقدر الذي يتناسب مع مقتضيات المرحلة، فإن يوري بيلوأوسوف نائب وزير الدفاع أشار في الاجتماع الذي عقده بوتين لمناقشة هذه القضايا، إلى أن روسيا قد تعمل على إنشاء منظومتها الشمولية الخاصة بالضربة الخاطفة الفائقة السرعة، لكنها سوف تنطلق في ذلك من عقيدتها الدفاعية لتطوير قواتها المسلحة. وكشف بيلوأوسوف عن أن منظومة الضربات الشمولية للرد السريع التي تجري الولايات المتحدة تجاربها عليها، تنص على توجيه الضربات غير النووية الصوتية الضخمة من الأراضي الأميركية إلى أهداف متفرقة في مختلف أرجاء الكرة الأرضية خلال ما يقرب من ساعة واحدة. وقال إن خطورة هذه المنظومة تكمن في أنها ومن خلال الضربة غير النووية يمكن أن تنزع سلاح القوات النووية الاستراتيجية في غضون ساعة واحدة بعد إطلاقها.

ومن اللافت أن عسكريين روسا كشفوا عن أن روسيا تملك بالفعل ما يسمح لها بالرد على مثل هذه المنظومة الأميركية. وكان الجنرال يورى بالويفسكي رئيس الأركان السابق وأحد المشاركين في صياغة العقيدة العسكرية الروسية الحالية الصادرة في فبراير 2010، أشار في تصريحات نشرتها وكالة أنباء «ريا نوفوستي»، إلى أن ما تملكه روسيا بالفعل يمكن أن يسمى «منظومة الرد السريع»، وهو ما أكده قسطنطين سيفكوف رئيس أكاديمية القضايا الجيوسياسية الذي قال إن روسيا تملك بالفعل صواريخ على غرار «101) «X-الصواريخ الاستراتيجية المجنحة) بعيدة المدى المحمولة جوا، والقادرة على الوصول لمسافة 5 آلاف كيلومتر، فضلا عن أن روسيا تمتلك أيضا صواريخ باليستية قادرة على الوصول إلى الأهداف الأرضية، وهو ما يعني عمليا أن روسيا تملك اثنين من المكونات الأساسية للضربة السريعة بعيدة المدى.[1]

ونقل كذلك عن إيغور كوروتشينكو رئيس تحرير مجلة «الدفاع الوطني» وعضو المجلس الاجتماعي التابع لوزارة الدفاع الروسية ما قاله حول ضرورة تطوير منظومات الرد على ما تملكه الولايات المتحدة من أسلحة لتوجيه الضربات الشمولية الخاطفة. وأضاف كوروتشينكو أن روسيا يمكن أن تستخدم منظومات الدفاع الصاروخية «إس – 500» لإصابة ليس فقط الأهداف الجوية، بل وأيضا القريبة من الفضاء الكوني حتى ارتفاع 200 كلم عن سطح الأرض والتي تتحرك بسرعة 8 كيلومترات في الثانية. وقال بضرورة تطوير

[1]– نفس المرجع، ص 03.

إمكانات منظومات الإنذار المبكر لإطلاق الصواريخ الباليستية المجنحة للعدو المحتمل في أراضي روسيا الاتحادية.

المطلب الثاني: قوة العقيدة الروسية بقيادة فلاديمير بوتين (2009 – 2014).

أوّلا- عقيدة الأمن السيبراني الروسي.

العقيدة الروسية الجديدة التي أقرها الرئيس فلاديمير بوتين، تكشف أنه تمت إضافة بند جديد يخص تهديدات الأمن السيبراني في المجالين العسكري والاقتصادي، وهذا التهديد، يستهدف إضعاف القيم الأخلاقية التقليدية الروسية.

ووفقا للعقيدة الروسية الجديدة لأمن المعلومات، التي وقعها الرئيس الروسي فلاديمير بوتين يوم 6 ديسمبر، فإن إحدى التهديدات الرئيسية لروسيا تتمثل "بزيادة عدد الدول الأجنبية التي لديها تأثير على البنية التحتية لمعلومات الأغراض العسكرية في روسيا".[1]

تم نشر الوثيقة على موقع الإنترنت الرسمي الروسي للمعلومات القانونية. العقيدة التي صممت من قبل مجلس الأمن الروسي وضعت فورا قيد التنفيذ.

تفرض العقيدة الجديدة وجود قيود على الخدمات التي تخص وسائل النفوذ الإعلامي والنفسي التي تمارسها البلدان الأخرى بهدف زعزعة استقرار الوضع السياسي الداخلي في روسيا.

وتهتم الوثيقة بشكل خاص بعمل وسائل الإعلام الأجنبية وتأثيرها على الروس، في المقام الأول على الشباب في البلاد. وتشير الوثيقة إلى أن الهدف من هذا التأثير هو التأثير على القيم الثقافية والروحية، لتقويض المبادئ الأخلاقية والأسس التاريخية والتقاليد الوطنية.

أحد الأهداف الرئيسية لواضعي هذه العقيدة للأمن السيبراني، هو "الردع الاستراتيجي والوقاية من النزاعات العسكرية، والتي يمكن أن تنجم عن استخدام تكنولوجيا المعلومات".

---

[1]- مقال بعنوان: **ما الجديد في عقيدة الأمن السيبراني الروسي؟**، (مجلة KATEHON، 2016)، ص 01، على الرابط الموالي: http://katehon.com/ar/article/m-ljdyd-fy-qyd-lmn-lsybrny-lrwsy

ثانيا- تقييم العقيدة.

يقول أوليغ ديميدوف، وهو خبير في الأمن السيبراني، من مؤسسة بحثية مستقلة مقرها موسكو: "العقيدة في شكلها الحالي هي العقيدة الأفضل بما يخص التهديدات الموجهة للأمن العسكري والتكنولوجي في روسيا. على سبيل المثال، هي تعمل بشكل مؤكد على الحماية من-العمليات السيبرانية من قبل الأجهزة الخاصة الأجنبية، فضلا عن مكافحة النشاط الاستطلاعي الأجنبي في روسيا". وبشير الخبير إلى أن الحكومة الروسية أولت اهتماما خاصا لمواجهة "ثورات التويتر" الجديدة، كتلك التي حدثت في الشرق الأوسط في بداية العقد الحالي.

وأضاف ديميدوف "الربيع العربي يشير إلى ما فعله الفيسبوك والتويتر وغيرهما من وسائل التواصل الاجتماعي، مما يسمح بتهديد الاستقرار الاجتماعي والسياسي، والشيء الرئيسي هو أننا لم يكن لدينا نموذج فعال لمنع حدوث ذلك".[1]

من وجهة نظر ديميدوف، المذهب الجديد يحتوي على ثلاثة مشاكل تتعلق ببنية العقيدة.

أولا؛ دور القطاع الخاص وهو المشغل الرئيسي في البنية التحتية للمعلومات غير واضح. "عادة تقوم الشركات: مثل كاسبرسكي لاب وانفو ووتش ومجموعة IB-وغيرها بحماية هياكل الدولة الروسية من الهجمات على الإنترنت وهذا يجب أن يكون أولوية في هذه العقيدة."

ثانيا؛ من الضروري زيادة مستوى التفاعل الدولي مع منظمة شنغهاي للتعاون ومنظمة معاهدة الأمن الجماعي وكذلك مع حلفاء روسيا الآخرين.

وأخيرا؛ من الضروري التأكد من وجود التفاعل العملي بين المراكز الوطنية والمراكز القطاعية للرد على التهديدات. في روسيا توجد مراكز على المستوى الاتحادي، أمّا على المستوى القطاعي (فهي مرتبطة مع البنك المركزي) وعلى المستوى الخاص أيضا.

[1]- نفس المرجع، ص 02.

ويقول ديميدوف "ومن الضروري إجراء مزيد من التدريبات المشتركة والسيناريوهات أو الممارسات للتصدي للهجمات الإلكترونية الدولية الكبيرة التي يمكن أن تقوض في الوقت نفسه عمل العديد من الخدمات التي تقدمها الدولة".

ثالثا- نقطة التحول.

العقيدة ليست عملا معياريا وليس لديها تأثير مباشر. أنها مجرد خلق هيكل عظمي وأساس لوضع وثائق إضافية وما يترتب عليها.

يلاحظ ديميدوف أن "العقيدة سوف تساعد باعتماد قوائم العمل لمشروع القانون الأساسي للبنية التحتية للمعلومات الحرجة، والتي وضعت في عام 2013، بحيث يمكن الآن تغطية الثقوب التشريعية.

روسيا تغيرت جذريا بشأن الأمن السيبراني بعد عام 2010، عندما ضربت جهات خاصة أمريكية وإسرائيلية المنشآت النووية الإيرانية في سياق عملية "ستكسنت"، كما يقول رئيس تحرير مجلة الدفاع الوطني إيغور كوريتشنكو.

ويضيف كوريتشنكو "ونتيجة للتأثير الخارجي، دخلت أجهزة الطرد المركزي لتخصيب اليورانيوم في البلاد حالة حرجة وانهارت بشكل جماعي". وحسب كوريتشنكو، فقد أخّر هذا الهجوم تطوير البرنامج النووي الإيراني ثماني سنوات[1] .

في 2 ديسمبر2013 أعلن جهاز الأمن الفيدرالي الروسي بأن هجمات على القطاع المصرفي في روسيا قد تنفذ من قبل الأجهزة الغربية، وإن كان قد تم الكشف عن تهديد واحد فقط حتى الآن، فإن هجمات أخرى قد تحدث في أي وقت.

---

[1]– نفس المرجع، ص 03.

الفصل الثالث: العقيدة الروسية في مواجهة التهديدات السيبرانية.

تمهيد الفصل الثالث:

تتّسم العلاقات الدولية بالديناميكية والتغير في ميزان القوى، فقد شهد العالم بعد الحرب الباردة تطورا كبيرا في المسائل المتعلقة بالأمن،حيث عرفت روسيا مجموعة من التهديدات الأمنية التي أثرت على أمنها واستقرارها، مما جعلها تعمل على تطوير عقيدتها الأمنية من خلال وضع مجموعة من السياسات والاستراتيجيات من أجل التفاعل مع التهديدات السيبرانية. حيث يعد الفضاء السيبراني من أهم التحديات التي تواجه روسيا على جميع الأصعدة الأمنية والسياسية من خلال بناء جيش سيبراني واتخاذ كل التدابير اللازمة للحد من الهجمات السيبرانية على روسيا.

المبحث الأول: المبادرة الروسية للتصدّي للهجمات السيبرانية.

المطلب الأول: الأمن السيبراني أحد الأسلحة الإستراتيجية.

إنّ الأمن السيبراني هو سلاح استراتيجي بيد الدول، فقد أصبحت الحرب السيبرانية جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات العابرة للحدود. وأصبح صناع القرار في دول العالم يصنفون وسائل الأمن السيبراني كأولوية في سياساتهم الدفاعية الوطنية، وأصبحت جزء لا يتجزأ من مهام أجهزة الأمن الوطنية[1].

وكان الرئيس بوتين في مقابلة مع قناة "إن بي سي" التلفزيونية الأمريكية، في 10 مارس/2013من هذا العام، قد أعلن أن روسيا مستعدة لتوقيع اتفاق على الأمن السيبراني مع الولايات المتحدة. وأجاب بوتين، على سؤال المراسل حول التدخلات المزعومة في انتخابات في الولايات المتحدة، "نحن نطرح عليكم مفاوضات رسمية، وأنتم ترفضون. وماذا تريدون بعد ذلك؟ تريدوننا بأمر من الكونغرس، بالركض وإجراء التحقيقات؟ دعونا نجلس، ونوقع اتفاقا بشأن الأمن السيبراني ونقوم بتنفيذه. وكيف تريدون أن تجري الأمور على غرار ذلك؟ ليس هناك طريق آخر في إجراء الشؤون الدولية."

ولكن الغريب، أن أميركا التي ادعت، تزوير انتخاباتها من قبل الهاكرز الروس، وتعرضها ودول الأطلسي لهجمات سيبرانية روسية عديدة خلال العام الماضي، لا تسارع، وغير مهتمة أصلا لمناقشة الاقتراحات الروسية، وهذا يعطي انطباعا واضحا بأن هذه الاتهامات محض افتراء، أو ربما أنهم لا يخشون إيفانوف! فتأثيره قد يكون محدودا! أو أنها أول المستفيدين من الفوضى السيبرانية، فهي من يقوم بتشويش أجهزة الملاحة للطائرات وإسقاطها لمنع التقارب بين الشعوب، أو أن أميركا ودول الغرب منشغلة الآن بأمور أهم، ألا وهي لملمة جروحهم وإحصاء خسائرهم، بعد الهزائم الفادحة التي لحقت بهم وبتحالفهم الكوني بالحرب في سوريا، وفي باقي مناطق الشرق الأوسط. هذه الهزائم التي لن تمر دون انهيارات في دولهم، وهي النتيجة الحتمية لأي دولة تهزم بحرب عبر التاريخ.

---

[1]– ثائر الطائي، **الأمن السيبراني أحد الأسلحة الإستراتيجية**، (مجلة KATEHON الإلكترونية، 2019)، ص 01، على الموقع: http://katehon.com/ar/article/lmn-lsybrny-hd-lslh-lstrtyjy.

ولم يبقى شيء بيد أميركا، إلا الاتهامات السيبرانية غير المدعومة بالأدلة، ولذا أتى اتهام جديد، في 3 آب/أغسطس، وهو التدخل في الانتخابات النصفية المقررة في نوفمبر/تشرين الثاني المقبل، وعلى ما يبدو، فإن أميركا قد أصبحت "حائط نصيص" للروس!

فحتى وقت قريب، كانت أميركا تتهم القراصنة الصينيون بهجمات ضدها، أما الآن فقد أتى دور الروس لينالوا حصتهم من الاتهامات الأمريكية. وفي عام 2010 اشتركت أميركا مع إسرائيل، بضرب المنشآت النووية الإيرانية بواسطة هجمات إلكترونية، في سياق عملية "ستكسنت"، وبنتيجتها دخلت أجهزة الطرد المركزي لتخصيب اليورانيوم في إيران حالة حرجة وانهارت بشكل جماعي.

إن الاتفاقيات الدولية لحماية الفضاء الرقمي ضرورية، حيث أنها بالأساس تضع حواجز أمام الدول لا ينبغي تجاوزها وتشريعات قانونية لمحاسبة المتجاوزين، فتشكل نوعا من الردع لهذه الهجمات، ولكن علمنا التاريخ، أن الاتفاقيات الدولية لا تنفذها إلا الدول الضعيفة، فجميع الدول إذا ما حشرت بالزاوية الضيقة، واحتاجت لضرب الاتفاقيات الدولية عرض الحائط، فإنها سوف تفعل.

كما إن التجسس قديم قدم التاريخ، ولطالما لجأت الدول لهذه الوسائل مع خصومها، فلذلك يجب تطوير استراتيجية وطنية للأمن السيبراني، وحماية البنية التحتية للمعلومات الحساسة، وذلك من خلال تحصين الأنظمة الإلكترونية للمنشآت المهمة في ملاجئ خاصة، وحمايتها بالحائط الناري Firewall يكون مزودا بأنظمة ذكاء اصطناعي، قادرا على مهاجمة الأعداء قبل شروعهم بالهجوم، فالهجوم خير وسيلة للدفاع، وكذلك له إمكانية تغير كلمات السر، ووسائل دفاعه الأخرى، وبرمجته، بشكل دوري وأوتوماتيكي، بحيث يمنع الاختراق[1].

كما لابد من توفير الحماية الكهرومغناطيسية للمعدات الإلكترونية المهمة بوضعها بما يشبه الصندوق الأسود في الطائرات، أو بتوفير وسائل دفاع لها من هذه الموجات، ويفضل أن تكون أنظمة تشغيلها بالكامل وطنية، وأما ما يتم استيراده، فيفترض تزويد الدولة بكل الثغرات والأبواب الخلفية لأنظمة التشغيل وتحميل الدول الموردة مسؤولية أي اختراق غير طبيعي، ويفترض فصل الأنظمة الحساسة عن الأنترنت، كما يحتاج لاتخاذ إجراءات لتنظيف وإعادة برمجة الأنظمة قيد العمل حاليا. وقبل هذا وذاك، يحتاج لتطوير الكوادر العاملة

[1]- **ثائر الطائي**، نفس المرجع، ص 03.

لحماية الأنظمة، والحيلولة دون الاشتراك "غير المقصود" بهذه الاختراقات، وكيفية التعامل ومعالجة هذه الهجمات.

المطلب الثاني: تنامي التهديدات السيبرانية.

في ضوء التطور التكنولوجي المتسارع وتنامي دور الفاعلين من نشطاء وجيوش إلكترونية وفواعل من دون الدول في المجال السيبراني، زادت التهديدات الإلكترونية بصورة شملت ليس فقط المواقع والخدمات الإلكترونية المدنية، ولكن أيضا البيانات والمنشآت العسكرية، بالإضافة إلى البنية التحتية الحرجة كالمفاعلات النووية، وهو تطور يفرض تحديات على الأمن القومي للدول[1].

ويسعى هذا التحليل لإلقاء الضوء على مفهوم الدفاع الإلكتروني من واقع الاستراتيجيات العسكرية المختلفة، وآليات تحقيقه، بالإضافة إلى الوقوف على أهم أهداف الدفاع الإلكتروني والمؤسسات المسؤولة عن تحقيقه في هذا المجال، وتحديد أبرز التطورات التكنولوجية التي أحدثت تقارب بين المجالات المدنية والعسكرية، وما فرضه ذلك من تحديات أمنية تسعى الدول لمواجهتها.

أولا: الدفاع الإلكتروني في الاستراتيجيات العسكرية.

يقصد بالدفاع الإلكتروني "مجموعة القدرات النظامية التي تمتلكها القوات المسلحة للحماية من تأثيرات الهجمات الإلكترونية، والتخفيف من حدتها والتعافي منها بسرعة[2]. وقد عرفت العقيدة الفرنسية الدفاع الإلكتروني على أنه" :مجموعة الوسائل الفنية وغير الفنية التي تسمح للدولة بالدفاع عن نظم المعلومات الحرجة في الفضاء الإلكتروني، وفي الإستراتجية النمساوية، فإن مصطلح الدفاع الإلكتروني يشير إلى جميع التدابير اللازمة للدفاع عن الفضاء الإلكتروني بالوسائل المناسبة لتحقيق الأهداف العسكرية الإستراتجية، ويعرفه البرلمان الأوروبي بأنه "عملية تطبيق الإجراءات الأمنية من أجل الحماية من الهجمات الإلكترونية والتعامل معها. وتستهدف تأمين البنية التحتية النظم الاتصالات والقيادة والسيطرة.

---

[1]– إيهاب خليفة، **مجتمع ما بعد المعلومات: تأثير الصورة الصناعية الرابعة على الأمن القومي**، (المستقبل للأبحاث والدراسات المتقدمة، العربي للنشر والتوزيع)، ص: 169، موقع إلكتروني: https://books.google.dz/books?id.

[2]– نفس المرجع، ص 169 – 170.

وفي الإستراتجية العسكرية البلجيكية، فإن الدفاع الإلكتروني هو "تطبيق تدابير وقائية فعالة للحصول على مستوى مناسب من الأمن الإلكتروني، وتقليل المخاطر الأمنية إلى مستوى مقبول، وباستثناء التعريف الأخير، فإن جميع التعريفات السابقة تطرقت إلى الدفاع الإلكتروني بمفهومه السلبي، والذي يعني القدرة على استقبال الهجمة الإلكترونية، وتلافي آثارها سريعا من دون الإضرار بالبنية التحتية والأهداف الإستراتجية للدولة، أما التعريف البلجيكي فقد أضاف بعدا جديدا وهو الدفاع الإلكتروني الوقائي أو الإيجابي، والذي يعني منع الهجمة قبل حدوثها، سواء من خلال اتخاذ تدابير وقائية أو هجمات إلكترونية إستباقية.

ومن مجمل التعريفات السابقة، يمكن تعريف الدفاع الإلكتروني الوقائي بأنه: "وسيلة التحقيق الأمن الإلكتروني من خلال استخدام آليات رصد الهجمات الإلكترونية وتحليلها وتحديد مصدرها والتخفيف من حدة آثارها على نظم الاتصالات والشبكات والبنية التحتية، وذلك في وقتها الحقيقي، مع توافر القدرات الهجومية لتعقب الكيانات وتدمير الشبكات، التي انطلق منها هذا التهديد.

ويختلف الدفاع الوقائي عن نظيره التقليدي في عنصرين رئيسيين، هما الاكتشاف المبكر للهجمات الإلكترونية، والأنية في التعامل معها حال حدوثها، فبينما يعمل الدفاع التقليدي كدرع داخلية للتخفيف من حدة الهجمات والتعافي السريع منها، يعمل الدفاع الوقائي كرمح استباقي الإعاقة الخصم عن تنفيذ الهجمة الإلكترونية. ويتحقق الدفاع الإلكتروني الوقائي من خلال ثلاثة أساليب رئيسية:

1- الكشف المبكر عن الهجمات في وقتها الحقيقي: وهو ما يتم من خلال استخدام حساسات (Sensors) على الشبكات والبرامج والتطبيقات، بالإضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يصنف على أنه هجمة إلكترونية، وبداية مواجهتها واحتوائها قبل أن تبدأ نشاطها في الشبكة أو النظم المستهدفة.[1]

2- الهجوم الإلكتروني الاستباقي: وذلك من خلال استخدام ونشر الديدان البيضاء (White Worms)، وهي برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمة إلكترونية محتملة، كما تقوم أيضا بتدمير أدوات وبرمجيات القراصنة، وهو ما يساعد في إحباط مخطط الهجمة

---

[1]- إيهاب خليفة، **تنامي التهديدات السيبرانية للمؤسسات العسكرية: cyber defence**، (أبوظبي: مركز الأبحاث والدراسات المتقدمة، 2017)، ص 55.

نفسها، وتحديد هوية ومصدر الهجمة، بما يمكن من إطلاق هجمة إلكترونية مضادة فيما يعرف بالاختراق العكسي.

3- التضليل والإخفاء والخداع: وهو ما يتحقق عن طريق إخفاء هويات الأهداف الإستراتيجية للدولة على الإنترنت، وتضليل الخصم أثناء محاولة الوصول إليها أو اختراقها، من خلال أدوات التمويه والخداع وتغيير ملامح الأهداف الإستراتيجية للدولة، بما يساعد على تضليل الخصم وتشتيت الانتباه عن الهدف الرئيسي.[1]

ثانيا: أهداف الدفاع في الفضاء السيبراني.

تتمحور أهداف الدفاع الإلكتروني في الحفاظ على مقدرات الأمن القومي التكنولوجي للدولة، من خطوط اتصالات وشبكات كمبيوتر وبنية تحتية، سواء مدنية أو عسكرية فضلا عن تأمين البيانات الحيوية، بما يساهم في النهاية في تحقيق الأمن الإلكتروني للدولة ويمكن تحديد أهداف الدفاع الإلكتروني في التالي:[2]

1- حماية الأهداف العسكرية: والتي تشمل تأمين نظم الإدارة والمراقبة ونظم التحكم والسيطرة ونظم توجيه الأسلحة وقطاع الاتصالات الحربية والأسلحة آلية القيادة، مثل الطائرات من دون طيار، فضلا عن حماية المنشآت العسكرية والحيوية مثل محطات الطاقة النووية من أي اختراق إلكتروني.

2- حماية البيانات العسكرية: والتي تشمل معلومات حول أفراد القوات المسلحة كالأسماء والرتب والمرتبات والوظائف داخل الجيش وأماكن الإقامة الشخصية، فضلا عن خطط التسليح وتصميمات الأسلحة، وخرائط انتشار القوات وتوزيع الأسلحة.

3- حماية البنية التحتية الحرجة: مثل قطاع الاتصالات والمواصلات ومحطات الطاقة وقواعد البيانات الحكومية وخدمات الحكومات الذكية والبنوك والمؤسسات المالية.

4 دعم وحدات الحرب الإلكترونية: وهي تلك الوحدات الخاصة بإدارة الحروب السيبرانية للدولة، حيث تكون مهمة الدفاع الإلكتروني هي تأمين الخطوط خلف هذه الوحدات، بما يحمي أهداف الدولة

---

[1]- إيهاب خليفة، **تنامي التهديدات السيبرانية للمؤسسات العسكرية: cyber defence**، ص 55.

[2]- نفس المرجع، ص 55.

الإستراتيجية في حالة شن هجوم إلكتروني مضاد عليها، وتوفير غطاء إلكتروني للوحدات المقاتلة بهدف التمويه والخداع وصعوبة تعقب مصدر الهجمة.

5- تحقيق الردع الإلكتروني: وذلك من خلال رفع تكلفة الهجوم الإلكتروني للدولة المعتدية، عبر إنشاء نظم دفاع إلكترونية صعبة الاختراق تحتاج إلى وقت وجهد كبيرين لاختراقها، مع تطوير قدرات تتبع الهجمات الإلكترونية واكتشاف مصدرها بما يؤدي في النهاية إلى التأثير على قرارات الخصم وردعه عن شن هجمات إلكترونية على الدولة في النهاية.

ثالثا: مؤسسات الدفاع الإلكتروني.

أجرى مكتب الأمم المتحدة لشؤون نزع السلاح دراسة مسحية في عام 2012 على الدول الأعضاء في الأمم المتحدة البالغ عددها حوالي 193 دولة، فوجد أن من بينها 114 دولة لديها برامج وطنية للأمن الإلكتروني، وأن 74 دولة منها أولت مهمة تحقيقه للقوات المسلحة، بينما قامت 67 دولة بإناطة مهمة الأمن الإلكتروني لمؤسسات مدنية لديها.[1]

وبصورة عامة، فإن مهمة تحقيق الدفاع الإلكتروني تقع على عاتق عدد من المؤسسات، وذلك على النحو التالي:

1- الجيوش الإلكترونية: حيث اتجه كثير من الدول حول العالم الإنشاء جيوش إلكترونية وفرق للعمليات عبر الفضاء الإلكتروني داخل صفوف قواتها المسلحة، تتكون من قراصنة معلومات مهمتهم اختراق شبكات الكمبيوتر الخاصة بالخصم، ونشر برامج التجسس والمراقبة، وتنفيذ المهمات العسكرية التي تطلب منها كتعطيل أحد البرامج العسكرية للخصم أو السيطرة على أحد الشبكات أو تدمير بعض الخدمات الإلكترونية، فضلا عن الدفاع عن الشبكات القومية وحمايتها من أي محاولة اختراق.

2- فرق الاستجابة الفورية للطوارئ (Computer Emer gency Response Team): وتعرف اختصارا باسم (CERT) وهي فرق مدنية، تكون مهمتها التحقيق في الأدلة الجنائية الرقمية، ومحاولة تتبع مصدر الهجمات والمتورطين فيها، وعادة ما يوجد بالدولة أكثر من فريق

---

[1]- إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية: cyber defence، ص 55.

استجابة للطوارئ، يتبع بعضها الوزارات، مثل وزارة الاتصالات، ويتبع البعض الآخر الشركات الكبرى، سواء كانت حكومية أو غير حكومية كشركات النفط والطاقة والاتصالات.[1]

3- كبريات شركات الاتصالات: هي أيضا أحد خطوط الدفاع الإلكتروني للدولة، وذلك بسبب امتلاكها قواعد بيانات خاصة بعدد كبير من المستخدمين داخل الدولة، كما تقع عليها مسؤولية تأمين جميع اتصالات الأفراد بالدولة، وضمان الحفاظ على سريتها وخصوصيتها من دون أن تتعرض للاختراق أو التسريب.[2]

4- القوات المسلحة التقليدية: قد تشارك بعض فرق القوات المسلحة التقليدية أيضا في عمليات الدفاع الإلكتروني، حيث تستدعى بعض العمليات الإلكترونية التدخل العسكري التقليدي من قبل القوات المسلحة، لتدمير خطوط اتصالات أو مراكز إدارة عمليات قرصنة تابع للخصم أو تدمير أسلحة خرجت عن السيطرة بسبب اختراقها.[3]

رابعا : قواسم مشتركة بين العسكري والمدني

بمرور الوقت حدث تقارب بين شبكة الإنترنت المفتوحة والشبكة العسكرية المغلقة، حيث أصبح بالإمكان الحصول على معلومات عسكرية من شبكة الإنترنت المفتوحة، بالإضافة إلى ظهور مجال مشترك بين الشبكة العسكرية والشبكة المفتوحة بفضل التطورات التكنولوجية، وهو ما زاد من التهديدات النابعة من الفضاء الإلكتروني، ويمكن توضيح ذلك في التالي:

1- استخدام بعض خدمات الإنترنت المدنية في الأغراض العسكرية: حيث قامت بعض الدول، مثل الولايات المتحدة الأمريكية و غيرها، بالاعتماد على تقنيات "الحوسبة السحابية" (Cloud Com puting) لتسهيل عملية إدارة جنودها وقواعدها العسكرية في مناطق متفرقة حول العالم، وذلك بالتعاون مع شركة "آي بي إم" (IBM) وشركة أمازون، نظرا لما توفره هذه الخدمة من وقت وجهد وتكلفة في تقديم الخدمات والمعلومات التي تتطلبها الإدارة اللامركزية لقواتها في أماكن متفرقة حول العالم، مع الاحتفاظ بدرجة

---

[1] - إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية: cyber defence، ص 55.

[2] - نفس المرجع، ص 55-56.

[3] - نفس المرجع، ص 56.

عالية من تأمين البيانات، ولم يقتصر استخدام الخدمات السحابية على جمع وتحليل وإتاحة المعلومات للجنود في الغرف المغلقة وحسب، بل أيضا تمت إتاحته للمقاتلين العسكريين في ميدان المعركة، حيث يتم جمع المعلومات المحيطة بمكان وظروف المعركة وتحليل المعلومات العملاقة (Big Data) بصورة| تساعد في تقديم أفضل سيناريو للمعركة إلى المقاتلين في الوقت الحقيقي.

2- الحصول على معلومات عسكرية باستخدام خدمات الإنترنت المدنية: فمثلا يمكن الحصول على صور المواقع عسكرية من خلال "خرائط جوجل وخدمات جوجل إيرث (Google Earth)، والتي تتيح للمدنيين الحصول على صور فورية للقواعد العسكرية بكل سهولة ويسر، كما يقوم بعض الجنود بوضع بياناتهم الشخصية على صفحات الإنترنت ومواقع التواصل الاجتماعي، وهي التي من خلال تحليلها يمكن الوصول إلى معلومات عسكرية مهمة، مثل رتب الجنود وأماكن إقامتهم وشبكة علاقاتهم الشخصية وزملائهم من أفراد القوات المسلحة.

3- دمج تقنيات عسكرية في بعض الأجهزة المدنية: ومن الأمثلة على ذلك نظم تحديد المواقع الجغرافي(GPS) ، حيث كانت قاصرة في بدايتها على الاستخدامات العسكرية فقط، لكن بمرور الوقت، ومع الحاجة إليها في الاستخدامات المدنية، أصبح كل شخص معه هاتف ذكي تتوافر فيه هذه الخاصية بصورة تقترب كثيرة من تلك المستخدمة في العمليات العسكرية، مما يعني قدرة الحركات المتطرفة على استخدام بعض التقنيات المدنية، مثل الدرونز التجارية وتحميلها بمواد متفجرة وتوجيهها عبر نظام (GPS) لاستهداف شخصيات عامة أو قواعد عسكرية.

4- الاعتماد على القطاع الخاص في القيام ببعض المهام العسكرية: حيث تلجأ وكالة الأمن القومي الأمريكي وبعض المؤسسات العسكرية في دول مختلفة إلى التعاقد مع مقاولين من الخارج والتعامل مع كثير من الشركات الخاصة للقيام ببعض المهام، مثل توريد أجهزة أو تأسيس شبكات أو بناء نظم أمنية ونظم اتصالات أو غيرها من الأعمال، وقد يؤدي ذلك إلى حدوث بعض الثغرات الأمنية داخل المؤسسات العسكرية. [1]

[1]- إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية: cyber defence، ص 56.

ولذلك أصبح هناك مجال مشترك على الإنترنت يجمع بين الاستخدام المدني والعسكري، وقد شكل هذا المجال نقطة ضعف داخل صفوف القوات المسلحة، تزامنت مع نقطة ضعف أخرى، هي تطور تقنيات الهجوم الإلكتروني على الشبكات العسكرية المغلقة، فتزايدت التهديدات الإلكترونية للقوات المسلحة، وأصبح من الضروري الاهتمام بالدفاع الإلكتروني كأحد أبعاد الدفاع بصورة عامة.

خامسا : التحديات الأمنية الرئيسية.

نتيجة لاقتراب الخطوط الفاصلة بين شبكة الإنترنت العادية والشبكات العسكرية من ناحية، مع تطوير القدرات الهجومية في مجال الحروب الإلكترونية، يتعرض الدفاع الإلكتروني العدد من التحديات الرئيسية، والتي يمكن تحديدها في التالي:

1– استهداف البنية التحتية الحرجة للدولة: إذ يتم استهداف البنية التحتية للدولة، سواء كانت مدنية أو عسكرية بهجمات إلكترونية، مثل استهداف محطات الطاقة والوقود والخدمات المالية والمصرفية ونظم الاتصالات والمواصلات.

ومن أبرز الأمثلة على ذلك تعرض أوكرانيا خلال شهر يونيو 2017 لهجمة إلكترونية شملت محطات الطاقة، بالإضافة إلى المؤسسات المالية، وأحد أكبر مطاراتها.

وقد شهدت السنوات القليلة الماضية العديد من الهجمات الإلكترونية على بعض البنى التحتية الحرجة والمؤسسات العسكرية، مثل محطات الطاقة النووية، كما في قيام فيروس ستاكسنت بتعطيل حوالي ألف من أجهزة الطرد المركزي في منشأة لتخصيب اليورانيوم في ناتانز في وسط إيران في عام 2010، فضلا عن تعرض أنظمة الكمبيوتر لشركة كوريا الجنوبية للطاقة المائية والنووية التي تديرها الدولة لهجمات إلكترونية في ديسمبر 2014 ،واتهمت الولايات المتحدة روسيا بالتورط في شن هجمات إلكترونية على شبكات كمبيوتر في عدة محطات طاقة نووية.[1]

2– السيطرة على الأنظمة العسكرية: ويقصد بها قيام قراصنة محترفين أو جيوش نظامية إلكترونية بشن هجمات إلكترونية بغرض السيطرة على نظم القيادة والسيطرة عن بعد، الأمر الذي يؤدي إلى إخراج

---

[1]– إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية: cyber defence، ص 57.

بعض منظومات الأسلحة عن سيطرة القيادة المركزية، وإعادة توجيهها نحو أهداف داخلية أو ضد دول صديقة، كما يمكن أيضا السيطرة على الطائرات من دون طيار، أو الغواصات النووية في أعماق البحار، أو السيطرة على الأقمار الصناعية العسكرية في الفضاء الخارجي وإخراجها عن سيطرة الدولة التابعة لها هذه الأسلحة والمعدات. وتزداد خطورة مثل هذه الهجمات، في ضوء التطور التكنولوجي، واعتماد اللوجستيات ونظم القيادة والتحكم وتحديد الأهداف وإصابتها على برامج كمبيوتر وشبكات الاتصالات.

3- سرقة المعلومات والبيانات العسكرية أو التلاعب بها: من خلال اختراق قواعد البيانات العسكرية وسرقتها أو تزييفها أو تدميرها إلكترونية، حيث تسعى الهجمات الإلكترونية في هذه الحالة إلى اختراق الشبكات الخاصة بالمؤسسات العسكرية بهدف سرقة خرائط نشر أنظمة التسليح أو التصميمات الخاصة بالمعدات العسكرية، وقد انطلقت واحدة من أخطر الهجمات ضد أنظمة حواسب الجيش الأمريكي في عام 2008، من خلال وصلة "يو إس بي (USB) متصلة بكمبيوتر محمول تابع للجيش في قاعدة عسكرية موجودة في الشرق الأوسط، ولم يتم اكتشاف انتشار برامج التجسس في كل من الأنظمة السرية وغير السرية في الوقت المناسب، مما شكل ما يشبه جسرا رقمية، تم من خلاله نقل آلاف الملفات من البيانات إلى خوادم خارجية (Servers). وبالمثل تم استهداف أكثر من 72 شركة من بينها 22 مكتبة حكومية و13 من مقاولي قوات الدفاع بهدف سرقة معلومات حول الخطط والمباني العسكرية.

4 جمع معلومات اقتصادية إستخباراتية: وهو ما يتحقق عن طريق اختراق قواعد البيانات المالية والمصرفية وقواعد بيانات الشركات والبنوك وجمع المعلومات التي قد تؤثر على الأمن القومي للدولة، وكذلك من خلال التجسس على المسؤولين الماليين ووزراء المالية ورؤساء الشركات الكبرى، حيث أصدر الرئيس الأمريكي باراك أوباما أثناء فترته الثانية أوامره بوقف التنصت على مقري صندوق النقد الدولي والبنك الدولي، وذلك في إطار مراجعة أنشطة جمع المعلومات الاستخباراتية، وذلك في أعقاب التسريبات، التي كشف عنها المتعاقد السابق مع وكالة الأمن القومي إدوارد سنودن بشأن برامج لجمع كميات هائلة من البيانات عن حلفاء وأعداء الولايات المتحدة والمواطنين الأمريكيين.[1]

[1]- إيهاب خليفة، تنامي التهديدات السيبرانية للمؤسسات العسكرية: cyber defence، ص 57.

وفي الختام، يمكن القول إنه في ضوء تنامي التوتر والصراعات في العلاقات بين الدول، على المستويين الإقليمي أو الدولي، فإنه يتوقع أن تلجأ الدول إلى توظيف الحروب الإلكترونية كأدوات إضافية في إدارة صراعها مع خصومها، خاصة مع تنامي أدوار الفواعل المسلحة من دون الدول، وهو ما يؤشر إلى زيادة التهديدات النابعة من الفضاء السيبراني مستقبلا، مما يتطلب من الدول كافة اتخاذ إجراءات لضبط سلوكها في الفضاء الإلكتروني، فضلا عن تطوير قدرات دفاعية لتأمين نفسها في مواجهة تلك التهديدات

المبحث الثاني: أهداف الجيش السيبراني الروسي.

المطلب الأول: حرب المعلومات بين روسيا والغرب.

مأساة روسيا والمجموعة الغربية هي أنهم يتبعون نهج حروب الماضي ضد بعضهم البعض . منذ اندلاع الأزمة الأوكرانية عام 2013، بدأ استخدام مفهوم حرب المعلومات على نطاق واسع في روسيا وفي الغرب وبالطبع في أوكرانيا. ومع ذلك، المصطلح نفسه يقدم القليل جدا حول المشهد الذي يحدث في فضاء المعلومات، وخاصة حول الحرب الواسعة والغامضة والمعروفة باسم "الحرب الهجينة." بالتعريف، تتميز الحرب أساسا بعمل عدائي يستهدف الدولة المعنية بالحرب تنفذه جماعات مركزية. وتتضمن تدفقات المعلومات كميات كبيرة من المحتويات المعادية والمنتجة عن عمد بشكل احترافي، والمشكلة هي أن وسائل الإعلام اليوم لا يمكنها أن تتطابق مع المعايير المركزية بشكل كامل. حتى في وسائل الإعلام المملوكة للدولة، تكون العلاقة بين الجهة صاحبة التوجيه لخلق أجندة معادية وبين المحتوى علاقة متكلفة. إضافة لذلك فإن التطور الهائل في وسائل الإعلام الاجتماعي وصلت لدرجة حيث يمكن لكل مستخدم أن يعمل كمنبر إعلامي مع كل المحافظة على حقوقه الخاصة، والصلة بين الأجزاء الكلية الافتراضية والجنود الافتراضين في حرب المعلومات تصبح أقل وضوحا.

إذا لماذا تعتبر وسائل الإعلام المستقلة في كثير من الأحيان أكثر عدوانية بكثير من تلك الشبكات المملوكة للدولة؟ لماذا يتوق الناس لنشر الدعاية بمحض إرادتهم دون أي إكراه، مما قد ينتج عنه تأثير مضاعف؟ علم النفس وراء نشر الدعاية.[1]

للإجابة على هذا السؤال، ينبغي أن ننظر في عمق وعينا الجماعي، وعميقا جدا ما وراء التطورات السياسية الجارية. الذات الداخلية التي نحن بحاجة إلى أن نراقبها يمكن ربطها مع ما سماه سيغموند فرويد وإريك فروم وفي وقت لاحق ديفيد ريزمان "بالضمير"، والذي يمثل مجموعة أفكار وقناعات عقلية تشكلت من خلال الثقافة والتعليم، وكأن نوعا من اللاوعي الجماعي زرع نظام قيم في اللاوعي الفردي. الأفراد ينظرون لهذه القيم باعتبارها قيمهم. نجاح الأخصائي في الدعاية يكمن في القدرة على تحديد هذه القناعات العقلية

[1] - مقال إلكتروني، **حرب المعلومات بين روسيا والغرب.. استنزاف وتوجيه خاطئ للموارد**، (مجلة KATEHON الإلكترونية، 2019)، ص 01، على الموقع: http://katehon.com/ar/article/lmn-lsybrny-hd-lslh-lstrtyjy.

وإيصالها للناس مع الرسالة الإعلامية ذات الصلة. إذا تمت إصابة الهدف، فهذا سيقوي المجموعة العقلية الموجودة من قبل .

يرى السياسيون أن دورهم قد تغير من القدرة على التلاعب بالرأي العام ليصبحوا رهائن له. لقد وجدوا المهمة صعبة للغاية نتيجة لتغيير رسالتهم، ويجب أن يتكيفوا مع الشعاب المرجانية الموجودة، ولاسيما أن هذه "الشعاب" لديها تاريخ طويل جدا.

ومن الملفت للنظر أن نرى كيف أن تدفقات المعلومات ينظر إليها بطريقة مماثلة من كلا الطرفين. في الواقع كلا من روسيا والدول الغربية، ناهيك عن أوكرانيا، تعتبر نفسها ضحية حرب المعلومات. يصر كل طرف على أنه في موقف دفاعي من حيث السياسة الإعلامية، ويسعى فقط لمواجهة المعلومات المعادية. تميل كل الأطراف إلى المبالغة إلى حد كبير بإمكانيات خصومها من حيث حرب المعلومات ونتائجها. هم جميعا يحاولون خلق قضية سياسية من خلال التطورات مع التركيز على البعد السياسي أو من خلال التهويل. [1]

بالطبع، لابد من دراسة هذا من منظور أوسع على أنه مزيج من جهود متعمدة لتعزيز أجندة سياسية ومظهر من مظاهر اللاوعي الجماعي. بقدر ما تكون السياسة معنية، لكن الأشياء يجب أن تأخذ بعين الاعتبار بعض القضايا التي لم تحل بين روسيا والغرب في فضاء ما بعد الاتحاد السوفيتي. لا تزال المنافسة تميز هذه العلاقة، لعبة محصلتها صفر ومعضلتها الأمن. التطورات في فضاء المعلومات تذكرنا بالقضايا المتعلقة ببنية الأمن الأوروبي. أما بالنسبة بما يخص اللاوعي الجماعي، فمن المهم أن نضع في اعتبارنا الصدامات الخطيرة بين روسيا وجيرانها في أوروبا الشرقية والوسطى، وكذلك في فضاء ما بعد الاتحاد السوفيتي.

في حالة أوروبا الشرقية والوسطى، جميع البلدان تقريبا في اتجاه واحد في علاقتها مع روسيا أو الاتحاد السوفيتي. حقيقة أن النخبة السياسية المحلية تحاول التعامل مع هذه الخبرات وتنشيط الأساطير لا يعني أنها غير موجودة. هذا يزيد من تعقيد سياسة الاتحاد الأوروبي وتواصلها مع الهويات الحساسة والهشة من بلدان أوروبا الوسطى والشرقية. بالإضافة إلى وجود عقلية الضحية في جورجيا وأوكرانيا.

[1]– نفس المرجع، ص 01.

بل لعله أكثر أهمية أن نفهم أن روسيا أيضا عاشت صدمات وخبرات مؤلمة أيضا، إن لم تكن أكثر من ذلك. مع الاحترام لجيرانها في أوروبا الشرقية، الذين كانوا ضحية في المخطط الكبير من قبل اللاعبين الرئيسيين، حيث اقتصر دورهم ليشكلوا منطقة عازلة تفصل الغرب عن روسيا. أما في فترة ما بعد انهيار الاتحاد السوفيتي فقد تحولت هذه الفكرة باقتدار إلى محرك التوحيد الوطني داخل هذه البلدان.

في الواقع يمكن لنبضات المعلومات الواردة من داخل روسيا ومن خارجها أن تؤدي إلى نتائج لا يمكن التنبؤ بها.

الرسالة الغربية لم تتغير كثيرا منذ الحرب الباردة: الديمقراطية والدولة القومية الكاملة والسوق وسيادة القانون والحرية والمساواة أمام القانون، وغيرها مثل التسامح والتنقل عبر الحدود التي تمت إضافتها مؤخرا إلى هذا المزيج. وعموما هذا فكر متحرر. لكن بلدان أوروبا الشرقية والوسطى تظهر حماسا أكثر لهذه الرؤية من الولايات المتحدة وأوروبا القديمة في أعقاب الحرب الباردة. وتبدو هذه الرسالة مختلفة في كل بلد حسب الممارسة العملية من التعايش التحرري مع درجة أقل من الحرية الفردية ومراقبة أقوى من جانب الدولة. وقد شكلت هذه الرؤية عاملا رئيسيا لدول ما بعد الاتحاد السوفيتي.[1]

ومن المثير للاهتمام أن روسيا على عكس الاتحاد السوفيتي لم تقدم بديلا (ومع الدراسة الأعمق نجد أن التجربة السوفيتية في جوهرها غربية أيضا، لأنها تروج للتحرر والتنوير). في الواقع تفتقر روسيا إلى تقاليد ديمقراطية ناضجة، لأن القاعدة الراسخة أن القانون هو الشرط الأساسي لتطوير اقتصاد السوق. وروسيا لم تتنصل من القيم المستوحاة من الغرب. حتى القيم الوطنية التي تعتبر الآن وبشكل رسمي أساس للهوية الروسية هي من القيم الغربية المتجذرة في الفكر الغربي حول وجود الدولة القومية والأمة كمجتمع سياسي، وليس العرق كأساس.

ويبدو أن الرسالة الروسية تدور حول فكرة الغرب أساسا لكن الغرب يلعب بشكل غير عادل من خلال نشر الفوضى في الوقت الذي يدعو فيه إلى النظام. هذه الفكرة تنطبق على الأزمات الأوكرانية والسورية. وتماما كما فعل الاتحاد السوفيتي ، روسيا تتهم الغرب بأنه يتصرف بسوء النية ولكنها لا تشكل تهديدا وجوديا للغرب.

[1]– مقال إلكتروني، **حرب المعلومات بين روسيا والغرب.. استنزاف وتوجيه خاطئ للموارد**، مرجع سابق، ص 02.

من ناحية أخرى ظهرت قوة قادرة على تقديم البديل الذي يختلف جذريا عن المشروع الغربي ويتحداه علنا. الإسلام الراديكالي يعزز الرؤية المختلفة للعدالة والدولة والحرية والقيم الأساسية الأخرى. وهذا يشكل مأساة بالنسبة لروسيا والغرب معا وخاصة عندما يستمران في حروب الماضي ضد بعضهم البعض، ما يعزز القوة الإيديولوجية للإسلام الراديكالي.

هذا الصراع بين روسيا والغرب هو الوهم الذي لن يقود إلى أي مكان. لكن هذا الوهم يمكن أن يكون له تأثير خطير على السياسة الواقعية. ومن المرجح أن يظل "التهديد الروسي" هو القوة التي توحد أوكرانيا وجورجيا والعديد من البلدان الأخرى في أوروبا الوسطى والشرقية لسنوات قادمة. وسوف تواصل روسيا نظرتها لهذه الدول كدمى موظفة من "المركز" الغربي حيث تنشأ المؤامرات المعادية لروسيا. كل هذا يضمن المزيد من الأصوات للسياسيين ويشد الجماهير بشكل اكبر وبدرجات أعلى لوسائل الإعلام[1]. مفارقة أخرى تجب ملاحظتها أن التفاعل الحالي على الجبهة الإعلامية هو أمر رأسمالي بطبيعته. حتى وسائل الإعلام المملوكة للدولة لا تتحرك بأوامر سياسية أو توجيهات قادمة من المستوى الأعلى، ولكنها تتحرك لضرب وتر حساس لدى النخبة السياسية ولدى الجمهور. التغييرات من حيث العرض والطلب يمكن أن تضع حدا لهذه "الحرب الزائفة" للمعلومات. كما أنها يمكن أن تعني نهاية الرأسمالية[2].

المطلب الثاني: الردع السيبراني؛ المفهوم والركائز.

أولا: مفهوم الردع السيبراني:

يعرف الردع السيبراني على أنه ''منع الأعمال الضارة ضد الأصول الوطنية في الفضاء والأصول التي تدعم العمليات الفضائية.[3] ويرتكز الردع السيبراني على ثلاثة ركائز هي عماد إستراتيجية الدفاع السيبراني، تتمثل في: مصداقية الدفاع Credible Defense، والقدرة على الانتقام An Ability to Retaliate، والرغبة في الانتقام A Will to Retaliate .

---

[1]- نفس المرجع، ص 02.

[2] -http://katehon.com/ar/article/hrb-lmlwmt-byn-rwsy-wlgrb-stnzf-wtwjyh-khty-llmwrd

[3]- Orji, Uchenna Jerome, **Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States**, *Defence against Terrorism Review*, Vol. 6, No. 1, Spring & Fall 2104, pp. 31-46

الركيزة الأولى – مصداقية الدفاع: يتطلب الدفاع عن أنظمة المعلومات، وردع أي محاولة لاختراقها – من بين متطلبات أخرى – توافر أنظمة نسخ احتياطيةBackup Systems ، مما يعني أن أي هجوم ناجح عليها، لن يسفر عن التدمير التام لها أو الفقدان الكلي لما تحويه من معلومات؛ ورغم تزايد تكلفة هذا الحل إلا إنه الحل العملي الأكثر فعالية.

الركيزة الثانية – القدرة على الانتقام: لابد أن يتكبد المهاجم ضررًا يفوق ما وقع على المدافع من أضرار، ولكن هذا يتطلب القدرة على الانتقام وتنفيذ هجمة سيبرانية أو أكثر ضد المهاجم الأصلي، بعد التعرف عليه وهو صعب التحقق.

الركيزة الثالثة – الرغبة في الانتقام: فعلى المدافع أو من تعرض للهجوم أن يعلن عن رغبته في الانتقام من المهاجم، ذلك أن امتلاك القدرة على الانتقام لا تكفي بمفردها لردعه.[1]

ورغم إمكانية تعريف المفهوم، وتحديد ركائزه على المستوى النظري، إلا أن هذا التعريف لا يحظى بإجماع الدول على المستوى العملي، والمثال على ذلك هو الولايات المتحدة والصين؛ ففي الوقت الذي تفضل فيه الولايات المتحدة استخدام مصطلح الأمن السيبراني Cyber Security للتركيز على التكنولوجيات والشبكات والأجهزة الآلية، تفضل دول مثل الصين وروسيا استخدام مصطلح أوسع ألا وهو "أمن المعلومات Information Security"، ليشمل المعلومات التي تمر عبر الشبكات وكذلك التقنيات المعلوماتية. ودون معجم مشترك، سيستمر الخلاف بشأن كيفية استخدام الإنترنت، وسياسات الردع، وطبيعة الهجمات الواجب ردعها.

ثانيًا: الهجمات السيبرانية.

تتطلب دراسة الردع السيبراني، التعرض إلى أنواع الهجمات السيبرانية لتحليل طبيعة ما يمكن ردعه منها. فيمكن للهجمات السيبرانية أن تتسبب في دمار هائل يطول الأمن القومي للدول، ويمكنها أيضًا أن

[1]- Putten, Frans-Paul Van Der, Minke Meijnders & Jan Rood, D**eterrence as a Security Concept against Nontraditional Threats, Clingendael Monitor**, 2015, pp. 1-64, Available at:https://www.clingendael.nl/sites/default/files/deterrence_as_a_security_concept_against_non_traditional_threats.pdf.

تستهدف القيادة السياسية، والأنظمة العسكرية، والمواطنين العزل[1]، وبخاصة أنها تشمل مجموعات كاملة من الأساليب والأدوات التي يمكنها التأثير في الفضاء السيبراني.[2]

يمكن تعريف الهجمات السيبرانية بأنها ''فعل يُقوض من قدرات وظائف شبكة الكمبيوتر، لغرض قومي أو سياسي، من خلال استغلال نقطة ضعف ما تُمكن المهاجم من التلاعب بالنظام[3]. "فهدف أنظمة المعلومات هو إتاحة المعلومات وضمان سلامتها. ولذا، تهدف الهجمات السيبرانية – على العكس من ذلك – إلى سرقة المعلومات، أو انتهاك سريتها، أو تعديلها، أو منع الوصول إليها. ولعل أبرز أنواع الهجمات ما يلي:

- **الهجمات السرية** : وتعد أحد أنواع التجسس التقليدي باستخدام وسائل التكنولوجيا الفائقة؛ ولعل معظم الهجمات السيبرانية المتطورة التي أطلقت من قبل الدول القومية أو الجماعات الإجرامية تقع ضمن هذه الفئة. ولكن، لا يمكن تصور الرد بهجوم ساحق أو مدمر على التجسس السيبراني، مهما بلغت تداعياته على الأمن القومي. ودون التهديد برد واسع النطاق، ستهوى الركيزة الأساسية للردع، وسيفشل في منع الهجمات السيبرانية.

- **Integrity Attacks**: تصمم بعض الهجمات لتحقيق ميزة تكتيكية أو إستراتيجية عن طريق تخريب نظم معلومات الخصم المدنية أو العسكرية الهامة. فيمكن أن ينطوي التخريب على التلاعب بالبيانات داخل نظم المعلومات التي يمكن أن تشوه وعي العدو عن طريق نشر معلومات خاطئة داخل أنظمة ذكائه، أو إخفاء أنشطة محددة قد تكون تحت المراقبة.[4]

---

[1]- Solomon, Jonathan, Cy**ber Deterrence between Nation-States: Plausible Strategy or a Pipe Dream?, *Strategic Studies Quarterly* 5**, No. 1, Spring 2011, Available at: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA538310.

[2]- Stevens, Tim, **A Cyberwar of Ideas? Deterrence and Norms in Cyberspace**. *Contemporary Security Policy*, Vol. 33, No, 1, 2015, pp. 148–170.

[3]- Todd, Graham H., Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, *Air Force Law Review*, 64, No. 96, 2009, p. 65.

[4]- Wilner, Alex S, Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism, *Journal of Strategic Studies*, Vol. 34, No. 1, February 2011, pp. 3–37.

ج :**Availability Attacks**–هي تلك التي تسعى لإغلاق نظم المعلومات To Bring Information Systems Offline. وتكمن خطورة الهجمات طويلة المدى منها في ما تسببه من أضرار مدمرة على الاقتصاد، بتأثيرها على شبكة الاتصالات أو الكهرباء على سبيل المثال. أما الهجمات قصيرة المدى التي تستهدف جمع المعلومات الاستخبارية، فيمكن أن تحجب قدرة الدولة على رؤية التهديد السيبراني التقليدي أو واسع النطاق من خلال منع المدافعين من الوصول إلى البيانات أو المصادر الاستخباراتية الحيوية. وهكذا، يمكن أن تشكل تلك التهديدات خطرًا على الأمن القومي، ولذا يجب أن يتم ردعها.[1]

وعلى ضوء ما سبق، ترى الباحثة أن العالم سيشهد مزيدًا من الهجمات السيبرانية في الأعوام القليلة القادمة، وستصبح الأسلحة الهجومية أكثر ضراوة. وبخاصة أن الهجمات السيبرانية يمكنها أن تفعل أشياء لا يمكن للهجمات التقليدية أن تفعلها. ولذلك، النجاح في المجال السيبراني لا يتطلب الدفاع فحسب؛ فالردع لن يكون فعالًا ما لم يتم تبن قدرات سيبرية هجومية.[2]

ثالثًا: أبرز حالات الهجمات السيبرانية:

ساهم عديد من الأحداث الدولية الأخيرة في رفع وعي الدارسين وصناع القرار بشأن التهديدات السيبرانية، مع التركيز على إمكانية انطباق نظرية الردع في هذا المجال .([22])وتتمثل أبرز الحالات فيما يلي:

- **إستونيا – أبريل 2007** :بدأت سلسلة من الهجمات التي يطلق عليها DDoS attacksضد المواقع التي تديرها الحكومة الإستونية، وتسبب الهجوم في عرقلة ولوج المواطنين إلى بعض المواقع مثل موقع الحزب السياسي الذي ينتمي إليه رئيس الوزراء. من جهة أخرى، استُخدمت الروابط التي ترعاها الحكومة في تضليل المستخدمين، وإعادة توجيههم إلى صور للجنود السوفيت، واقتباساتٍ من مارتن لوثر كينج عن محاربة الشر.

[1]- Jarno Limnéll, Offensive Cyber Capabilities are Needed Because of Deterrence, *The Fog of Cyber Defence*, No. 200, 2013, pp. 200-207

[2]- Catherine Lotrionte, A Better Defense: Examining the United States New Norms-Based Approach to Cyber Deterrence, Georgetown Journal of *International Affairs*, 2013, pp. 71-84.

ب- جورجيا – أغسطس 2008 :شهدت جورجيا بالتزامن مع حربها ضد روسيا في أغسطس 2008 مجموعة من الهجمات السيبرانية، وإن كان ضررها الفعلي في حده الأدنى، من حجب بعض المواقع المستهدفة. ويتفق معظم المحللين على أن القوميين الروس هم المسئولون عن الهجوم، ولكن دون دليل يذكر.[1]

ج- كوريا الجنوبية والولايات المتحدة يوليو 2009 :تم استهداف مواقع البيت الأبيض، ووكالة الأمن القومي، والإدارة الاتحادية للطيران Federal Aviation administration ، ووزارة الخارجية، والخدمة السرية Secret Service ، والخزانة، ولجنة التجارة الاتحادية Federal Trade Commission ، فضلًا عن جهاز المخابرات الوطني في كوريا الجنوبية.

وكذلك الهجوم على شركة سوني بيكتشرز الأمريكية في عام 2014، بسبب فيلم من إنتاج هوليوود، عن زعيم كوريا الشمالية كيم يونغ أون. واستخدم فيروس ''ستكسنت'' – سابقًا- لمهاجمة برنامج إيران النووي في نوفمبر 2007، ويُعتقد أنه من تطوير الولايات المتحدة وإسرائيل، وقد تم اكتشافه في عام 2010.

وفي يوليو 2011، أعلن نائب وزير الدفاع ويليام لين أن أكثر من 24 ألف ملف من ملفات وزارة الدفاع قد سرق. قبل ذلك ببضعة أشهر، تم اختراق إحدى المختبرات العلمية الرئيسية التابعة لحكومة الولايات المتحدة، ولم تعلن الحكومة الأمريكية عن هوية مرتكبي الهجوم.

وفي عام 2012، تم تدمير 35 ألف جهاز كمبيوتر في شركة النفط السعودية ''أرامكو''، لتخريب صادرات النفط. وألقت المخابرات الأمريكية اللوم على إيران. وفي عام 2016، هاجم القراصنة إحدى الوكالات الحكومية السعودية، بالإضافة إلى منظمات في قطاعات الطاقة والصناعة والنقل، والهيئة العامة للطيران المدني التي تنظم الطيران السعودي.

وشهد عام 2016، التسلل الروسي إلى خوادم البريد الإلكتروني للجنة الوطنية الديموقراطية، كما تم اختراق البريد الإلكتروني الخاص بجون بوديستا رئيس الحملة الانتخابية الرئاسية لهيلاري كلينتون. وقام وسطاء بتسريب رسائل إلكترونية إلي موقع ويكليكس، وعلى إثرها قامت الولايات المتحدة بطرد 35 دبلوماسيًا روسيا.

[1]- Catherine Lotrionte, Opcit, pp. 71-84.

خامسًا: متطلبات الردع

الردع السيبراني صعب التنفيذ، كما أن هناك العديد من العوامل التي يجب أن تحدث لضمان تحقيق النتائج المرجوة منه، منها:[1]

- **تطبيق طرق ووسائل جديدة:**

يتطلب الردع السيبراني تطبيق طرق وأساليب جديدة، واعادة تكييف مفاهيم الردع التقليدية لتتناسب مع هذا المجال الجديد. فلا يمكن معرفة الهدف من الهجمات دون معرفة من شنها؛ ودون معرفة الخصم وهدفه، لا يمكن للردع أن ينجح، وسرقة المعلومات قد تتكرر مستقبلًا، ودون الرد على ذلك الهجوم لن يكون الردع ممكنًا لتآكل مصداقيته. ولذا تتعدد الخيارات والسبل المقترحة للردع، ولعل منها ما يلي:[2]

الخيار الأول – الردع السلبي :وهو الأقل تعقيدًا، لكنه ليس واقعيًا، إذ يتمثل في عدم الرد على الخصم، ولكن مع الاعتراف بأن الأمن السيبراني، وكافة الإجراءات المتبعة غير كافية، وتطوير الأنظمة الأمنية بشكل مستمر. فمن شأن أي تحسن في تدابير الأمن السيبراني أو الردع السلبي أن يرفع تكاليف أي هجوم سيبراني في المستقبل، مما يقلل من فرص حدوثه. ومع ذلك، سيعتبر المهاجم أن هذا الرد بمثابة دعوة لمواصلة الأنشطة السيبرانية على نطاق أوسع.

الخيار الثاني – الاحتجاجات الدبلوماسية :يمكن طرد مسئولي الدولة التي يشتبه في شنها الهجوم، ومع ذلك، تسرى قواعد المعاملة بالمثل على ذلك الأمر. ومن شأن ذلك أن يضر بسمعة الدولة على الصعيد الدولي، لكنه في المقابل لن يسبب لها ما يكفي من أضرار تردعها عن شن هجمات مستقبلية.

الخيار الثالث – التدابير القانونية :بمعنى اتخاذ إجراءات قانونية ضد الدولة التي يشتبه في شنها الهجوم. ولكن كما هو الحال مع الاحتجاجات الدبلوماسية، التدابير القانونية هي في الغالب ذات طبيعة

---

[1]– رغدة البهي، <u>**الردع السيبراني: المفهوم والإشكاليات والمتطلبات**</u>، (دبي: المركز العربي لأبحاث الفضاء الإلكتروني، 2017)، ص 3.

[2]– نفس المرجع ص 3–4.

رمزية، وتنطوي على خطر إقامة دعوى قضائية تضطر فيها الدول لكشف معلومات استخباراتية حساسة، ليسبب ذلك ضرراً أكثر مما يستحق، ولن يكون له تأثير رادع.

الخيار الرابع – العقوبات الاقتصادية :بعد إتهام الولايات المتحدة لكوريا للمشاركة في قرصنة شركة سوني بيكتشرز مثلًا، تم تعزيز العقوبات الاقتصادية ضد النظام الكوري. ومع ذلك، بمجرد تثبيت العقوبات أو تعزيزها، لن يكون لدى الدولة أي سبب وجيه لتغيير سلوكها، ما لم تكن هناك مبادئ توجيهية حول كيفية تخفيف أو التخلص من العقوبات. ناهيك عن التداعيات المحتلة للاعتماد المتبادل، وارتباط اقتصاديات الدول مع بعضها البعض في شبكة مترامية الأطراف، متداخلة المصالح؛ فمن شأن ذلك أن يطول الدول التي تفرض العقوبات أيضًا.

الخيار الخامس – الانتقام في الفضاء الافتراضي :لطالما كان التهديد بالانتقام رادعًا فعالًا يردع الاختراقات السيبرانية المستقبلية. فمن شأن سرقة ونشر معلومات الخصم واستهداف بنيته التحتية أن يكون خيارًا فعالًا. ومع ذلك، يتزايد خطر التصعيد المتبادل.

الخيار السادس – الانتقام العسكري :وهو خيار غير واقعي، لأنه سيسفر عن رد عسكري مضاد، ويمكن أن يبدأ عملية خطيرة من التصعيد. ويبدو هذا الخيار مرجحًا إذا أسفرت الهجمات السيبرانية عن نتائج كارثية، ووفقًا لموازين القوى بين طرفي الصراع. وتكمن الإشكالية في أن التهديد بضربة مضادة، قد لا يكون سريعًا بما يكفى لكي يمنع العدوان. ومع إشكالية الإسناد، قد تصبح الضربة المضادة آلية للرد والدفاع لا الردع.

كل من تلك الخيارات يمثل إشكالية إلى حد ما؛ فجميعها تقريبًا يشترك في خطر التصعيد، وأيا منها قد يعجز عن ردع الهجمات السيبرانية في المستقبل. ولكن إذا لم يتم اتخاذ أي إجراء، فإن مصداقية الأمن السيبراني ستتضاءل.[1]

وفي رؤية الباحثة، تعكس تلك الخيارات حقيقة هامة، تنال من مصداقية الردع، مفادها اللجوء إلى مجالات أخرى بخلاف المجال السيبراني للرد على الهجمات التي تطال ذلك المجال. فنظرًا لصعوبة تحديد المهاجم بدقة، قد لا يلجأ الطرف المتضرر إلى الرد على الهجوم عبر المجال السيبري، ولكن قد يلجأ إلى التهديد

[1]– رغدة البهي، مرجع سابق، ص 4.

باستخدام الأداة العسكرية ردًا عليه، أو قد يقرر استهداف أهداف مناظرة لدى الخصم؛ فإذا تسبب الهجوم السيبراني في تعطيل إمدادات الكهرباء على سبيل المثال، يمكن استهداف مثيلتها لدى الخصم، وإذا تسبب الهجوم السيبراني في ضرر بالغ يهدد الأمن القومي، فيمكن التهديد بتغيير النظام السياسي لدى الخصم أو شن الحرب عليه.

بلورة إستراتيجية متكاملة للردع:

يختلف الردع في عصر المعلومات كثيراً عنه في عصر الحرب الباردة التي تميزت بقلة عدد الدول المالكة للأسلحة النووية، لكن عدد الدول التي تسعى لتطوير أسلحتها السيبرانية يبلغ 140 دولة، كما أدخلت 30 دولة الوحدات السيبرية في جيوشها.

الحديث عن الردع السيبراني بات أكثر مرونة، وباقترابات مختلفة، وتلك المرونة يمكن تداولها بطريقتين مختلفتين:

الأولى – الأنظمة البديلة: إن اعتماد دولة ما على نظام واحد، وتم اختراقه، سيسفر عن عواقب وخيمة؛ وبخاصة إذا تعلق هذا النظام بالبنية التحتية الرئيسية للدولة. لذلك، يمكن للدول خلق أنظمة بديلة لتكون في حوزة الدولة نفسها أو الدول الصديقة. وفي حالة حدوث هجوم سيبراني، يمكن الاستعانة بتلك الأنظمة البديلة أو الاحتياطية.

الثانية – إعادة التأسيس :فإذا أمكن للدولة التغلب على الهجوم الذي تعرضت له بسرعة، وإعادة تشغيل النظام، ستكون الآثار هامشية. ولكن الطريقة الوحيدة لتجنب الهجوم هي الاحتجاب عن الجميع، ورغم كونه السبيل الأفضل للردع، إلا أنه يكتنفه مسائل قانونية عدة.[1]

---

[1]– نفس المرجع ص 4.

المبحث الثالث: مستقبل الإستراتيجية الروسية في مواجهة التهديدات السيبرانية.

المطلب الأول: التعاون الروسي الأمريكي لمواجهة التهديدات السيبرانية.

بعد تنصيبه في عام 2009، أعلن الرئيس أوباما إعادة ضبط العلاقات بين الولايات المتحدة، وروسيا أو بدئها لعكس مسار الانجراف / الانزلاق الخطر) الذي كان قد اكتنف العلاقة أو شابها خلال رئاسة جورج دبليو بوش[1]. تهدف إعادة الضبط إلى تعميق الحوار الثنائي، وإشراك روسيا في مبادرات براغماتية ذات اهتمام مشترك، بمثل إقامة روابط أمنية، وتجارية أقوى، مع الحد من التوترات الناجمة عن غزو روسيا لجورجيا

أدت تصريحات إدارة أوباما تجاه روسيا إلى بعض الانتصارات المهمة في السياسة، إذ منحت روسيا الولايات المتحدة الإذن لنقل إمدادات القوات عبر أراضيها إلى أفغانستان، إذ أصبحت طرق الإمداد البديلة في أنحاء باكستان جميعها خطرةً خطرا متزايدا[2]. في عام 2010، وقع الرئيسان: أوباما وميدفيديف معاهدة الحد من الأسلحة الاستراتيجية الجديدة (ستارت)، إذ خفضت القيود على الرؤوس الحربية الاستراتيجية المسموحة الروسية والأميركية إلى الثلث[3]. وشاركت روسيا في أول مؤتمر قمة للأمن النووي الذي عقده الرئيس أوباما في عام 2010، وعملت مع الولايات المتحدة للتخلص من 17 ألف قطعة من البلوتونيوم الزائد من الأسلحة النووية.[4]

وفي ما يتعلق بالتعاون العسكري، تعهدت الدولتان بتطوير «علاقة استراتيجية جديدة تقوم على الثقة المتبادلة، والانفتاح، والقدرة على التنبؤ والتعاون»، وذلك جزئيا بتجديد العلاقات العسكرية العسكرية، من خلال مجموعة العمل المتعلقة بلجنة التعاون الثنائية حول الدفاع التي أسست حديثا بين الولايات المتحدة وروسيا.

---

[1]- البيت الأبيض، مكتب السكرتير الصحفي، "**العلاقات بين الولايات المتحدة وروسيا: ورقة حقائق** "إعادة تعيين"، بيان صحفي من البيت الأبيض، 24 يونيو/حزيران 2010.

[2]- ريتشارد أ. أوبل، **الولايات المتحدة تؤمن طرق توريد جديدة إلى أفغانستان**، صحيفة نيويورك تايمز، 20 كانون الثاني، يناير 2009.

[3] -http://www.nytimes.com/2009/01/21/world/asia/21pstan.html

[4]- المرجع نفسه.

المطلب الثاني: دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية.

ارتبط تصاعد الصراع بين روسيا والدول الغربية بقيادة الولايات المتحدة، خلال السنوات الماضية، باستدعاءٍ متنامٍ لحرب المعلومات Information Warfare كأحد المداخل المهمة للتأثير في مسارات الصراع. ففي خضم التنافس على قيادة النظام ؛ تَشَكَّلَ توجُّهٌ استراتيجي مغاير لدى موسكو، له امتداداته التاريخية في الحقبة السوفيتية.

هذا التوجه مفاده أن الانتصار في الصراع مع الغرب لن يتحقق بالاعتماد القاصر على الأدوات العسكرية التقليدية، ولكن الأمر يتطلب تفعيل أدوات الحرب المعلوماتية وغيرها من الأدوات غير التقليدية، وهو ما أطلق عليه رئيس هيئة الأركان العامة الروسية «فاليري جيراسيموف» نهجًا مختلفًا لتحقيق الأهداف السياسية والعسكرية الروسية من خلال «الطرق غير المباشرة وغير المتماثلة».

وفي إطار تلك الحرب، وُجهت اتهامات لروسيا باستعمال وسائل التواصل الاجتماعي للترويج لأخبار كاذبة كان لها تأثير كبير في نتائج الانتخابات الرئاسية الاميركية التي أُجريت في الثامن من نوفمبر الماضي، وإن كانت موسكو تنفي تلك الاتهامات. وفي ١٠ أكتوبر الجاري، كشف تقرير لصحيفة «نيويورك تايمز» عن قراصنة مقربين من الحكومة الروسية استخدموا برمجيات لمكافحة الفيروسات من إنتاج شركة «كاسبرسكي لاب» لسرقة أسرار وكالة الأمن القومي الاميركي. وقد سبق أن أمرت وزارة الأمن الداخلي الأميركية في سبتمبر الماضي الوكالات الحكومية بإزالة جميع برامج «كاسبرسكي» من أجهزة الكمبيوتر، بسبب المخاوف الأمنية[1].

أوّلا- حرب المعلومات:

صدرت في عام 2012 وثيقة وزارة الدفاع الروسية المعنونة «مفهوم الأنشطة الفضائية للمعلوماتية للقوات المسلحة بالاتحاد الروسي The Russian Federation Armed Forces Information Space Activities Concept، لتكشف عن الحيز الهام الذي تمثله المعلومات في الإطار الاستراتيجي الروسي، وتبنت

[1]- محمد بسيوني، **عقيدة جيراسيموف: دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية**، (المستقبل للأبحاث والدراسات المتقدمة، مجلة إلكترونية، 2017)، ص 01.

الوثيقة تعريف فضاء المعلومات بأنه «مجال النشاط المتصل بتشكيل المعلومات ونقلها واستعمالها وتخزينها، مما يؤثر على الوعي الفردي والمجتمعي، فضلًا عن المعلومات في معناها الضيق، وكذلك الهياكل الأساسية للمعلومات.

في عام 2013، نشر الجنرال الروسي رئيس هيئة الأركان العامة الروسية «فاليري جيراسيموف» مقالًا عن التحديات الجديدة وأساليب تنفيذ العمليات القتالية، وكان هذا المقال بمثابة تأسيس لما يُعرف في الغرب بـ»عقيدة جيراسيموف«The Gerasimov doctrine ، وهذه العقيدة تنطوي على مجموعة من الأفكار بشأن الأدوات غير التقليدية في الحروب الراهنة، والتي تتضمن أدوات مختلفة من بينها المعلومات، سواء من خلال الفضاء الإعلامي أو الفضاء الإلكتروني، واستهداف نقاط الضعف للخصوم، وتجنب المواجهة العلنية حتى المراحل النهائية للصراع.

لقد كان «جيراسيموف» يُعبّر عن أطروحةٍ تَزَايَدَ استحضارها في روسيا خلال السنوات الماضية، مع سعي موسكو الحثيث لاستعادة إرثها التقليدي كقوة مؤثرة في النظام الدولي، وما يستلزمه ذلك من توظيف أدوات الحرب المعلوماتية. وفي هذا السياق، اعتمدت روسيا في ديسمبر ٢٠١٦ وثيقة «عقيدة أمن المعلومات في الاتحاد الروسي Doctrine of Information Security of the Russian » Federation، وأكدت الوثيقة البُعدَ العسكري لمسألة المعلومات كأساس لأمن الدولة، وتُحدد «أسلحة المعلومات» بوصفها إحدى الأدوات لتحقيق الأهداف السياسية.

وكان من شأن هذه الأطروحات شرعنة استعمال مجموعة واسعة من الأنشطة والعمليات التي تسعى إلى التلاعب أو تشويه أو سرقة أو خلق أو تدمير المعلومات وإعادة إنتاج الروايات المضللة لخدمة المصالح الروسية، أو بمعنى آخر فإن هذه الأنشطة والأدوات غير المتناظرة تجاوز أو -على أقل تقدير- تحيد القدرات الغربية العسكرية، وتستغل الثغرات في المجتمعات الغربية[1].

---

[1]- محمد بسيوني، نفس المرجع، ص 02.

ثانيا- الأدوات الروسية:

يعتقد ديفيد سميث David J. Smith في دراسة له بعنوان «كيف تستخدم روسيا الحرب السيبرانية؟»، أن روسيا «تعتمد على مفهوم واسع للحرب المعلوماتية، يشمل: الاستخبارات، والتجسس المضاد، والخداع، والتضليل، والحرب الإلكترونية، وتدمير الاتصالات وأنظمة دعم الملاحة، والضغوط النفسية، إضافة إلى الدعاية وإلحاق الضرر بنظم المعلومات».

ووفقًا لهذه الرؤية تبدو الحرب المعلوماتية الروسية مستندة بنحو جوهري إلى أداتين رئيستين:
1- التضليل المعلوماتي: ينبني هذا المدخل على كيفية توظيف الأدوات الإعلامية والدعائية المختلفة بهدف إعادة إنتاج روايات مضللة للآخرين، ومشوهة للحقائق، تُضعف روايات الأطراف الغربية المناوئة، وتخدم في نهاية المطاف المصالح الروسية. وقد تجلّى هذا النمط أثناء تعاطي وسائل الإعلام الروسية مع الأحداث السياسية التي شهدتها الدول الغربية.

لقد تحدثت العديد من التقارير الغربية عن حملات تضليل مارستها روسيا أثناء الانتخابات الرئاسية الاميركية في عام 2016 من خلال وسائل الإعلام الروسية، وفي مقدمتها شبكة تليفزيون «روسيا اليوم»، حيث سعت الشبكة إلى تشويه صورة المرشحة الديمقراطية «هيلاري كلينتون»، واتهامها بالفساد، والعلاقة مع المتطرفين الإسلاميين، ناهيك عن التركيز على الرسائل الإلكترونية التي تم تسريبها للمرشحة، وتنفي موسكو تلك الاتهامات.

وتكرر هذا النموذج في الانتخابات الرئاسية الفرنسية في عام 2017؛ إذ منعت حملةُ الرئيس الفرنسي «إيمانويل ماكرون»، المحسوب على تيار الوسط، ممثلي شبكة تليفزيون «روسيا اليوم» ووكالة «سبوتنيك» الروسية من الدخول إلى مقراته، وبرر المتحدث باسم الحملة هذا المنع «بتعمد كلا الجهتين إصدار أخبار وهمية ومعلومات كاذبة للإضرار بماكرون».[1]

1- القرصنة الإلكترونية: يُشكّل الهجوم على البنية المعلوماتية للدول الأخرى جزءًا هاما من استراتيجية حرب المعلومات الروسية، باعتباره وسيلة للحد من فعالية الخصم، وإرباكه وتضليله، ناهيك عن فعالية

[1]- محمد بسيوني، نفس المرجع، ص 2-3.

عمليات القرصنة في تجزئة نظام القيادة لدى القوى المناوئة لموسكو، والسيطرة عليها ولو حتى لفترة زمنية محدودة.

وعلى الرغم من نفي موسكو تورطها في عمليات القرصنة الإلكترونية التي تعرضت لها الدول الغربية خلال السنوات الماضية؛ إلا أن هذه الدول كثيراً ما كانت تؤكد التورط الروسي في هذا الشأن، لاسيما مع طبيعة الدول التي تعرضت لعمليات القرصنة والعلاقات التي تجمعها بروسيا، ناهيك عن الجماعات التي أعلنت ارتكابها عمليات القرصنة التي كانت في الغالب تحمل الجنسية الروسية.

ففي عام 2007، تعرضت أستونيا لهجمات قرصنة إلكترونية استهدفت عددًا من المؤسسات الحكومية والبنوك ووسائل الإعلام، وبدا من طبيعة الأحداث وسياقها الزمني تورط روسيا في الهجمات؛ إذ إن الهجمات تزامنت مع توتر في العلاقات بين روسيا وأستونيا عقب قرار الأخيرة إزالة نُصب تذكاري يعود للحقبة السوفيتية من العاصمة الأستونية تالين.

وقد تم استدعاء القرصنة الإلكترونية بصورة أكثر كثافة إبان الحرب الروسية الجورجية، وفي 7 أغسطس 2008 بينما كانت وحدات الجيش الروسي تعبر الحدود إلى جورجيا، اتهمت روسيا بشن هجوم سيبراني على مواقع الحكومة ووسائل الإعلام والمنظمات المالية والتجارية وغيرها في جورجيا.

وفيما كانت الدول الغربية تكثف من انتقاداتها واتهاماتها لروسيا، كانت موسكو تنكر التورط في عمليات القرصنة الإلكترونية، وفي الوقت ذاته كانت تصوغ انموذجًا جديدًا من العلاقات، يطلق عليه «تيم مور Tim Maurer «توظيف وكلاء سيبرانيينCyber Proxy Actors ، من منظمات ومجموعات للقرصنة تخدم مصالحها، وتسمح لها بالتنصل من الاتهامات الغربية.

ولعل أبرز هذه المجموعات مجموعة APT28 الروسية التي اتهمتها ألمانيا باختراق بيانات لنواب في البرلمان الألماني في عام 2015، واستعمال برامج خبيثة لمهاجمة العديد من الأجهزة المستخدمة من قبل النواب والموظفين. وفي العام ذاته هاجمت المجموعة قناة «تي في 5 موند» الفرنسية، وهو ما أدى إلى إيقاف بث القناة لساعات، والإضرار بأنظمتها[1] .

[1]- محمد بسيوني، نفس المرجع، ص 4.

وتمتلك مجموعة APT29 هي الأخرى قدرات وموارد متقدمة ومتطورة، دفع الكثيرين من المحللين الغربيين إلى افتراض وجود علاقة بينها وبين النظام الروسي، فضلًا عن استهداف المجموعة الكيانات للاستيلاء على المعلومات التي ترتبط ارتباطًا وثيقًا بالمصالح الجيوسياسية الروسية. وخلال السنوات الأخيرة ازداد تركيز المجموعة على أهداف استخباراتية متصلة بالصراع في أوكرانيا، وهو ما يتضمن مجموعة واسعة من المؤسسات الغربية، مثل: الحكومات، والأجهزة الأمنية، ومراكز الفكر والرأي.

وتُقدم مجموعة Cyber Berkut نموذجًا آخر لمجموعات القرصنة الموالية لروسيا، وارتبط بزوغ المجموعة بتطورات الصراع داخل أوكرانيا، حيث تتبنى المجموعة خطابًا معاديًا للغرب، ومواليًا لموسكو بنحو أو بآخر. وقد نفذت المجموعة عددًا من الهجمات داخل أوكرانيا لعل أهمها في مايو 2014 حينما أعلنت مسئوليتها عن اختراق أنظمة لجنة الانتخابات المركزية الأوكرانية في الانتخابات البرلمانية على النحو الذي عطل أنظمة فرز الأصوات.

ثالثا- دوافع متعددة:

يفترض "بافل أنتونوفيتش Pavel Antonovich " أن «ترسيم الخطوط الفاصلة بين الحرب والسلام يمكن أن يتآكل بسهولة في الفضاء السيبراني، فيمكن أن يتم إلحاق أضرار، مهما كانت طبيعتها، بالخصم، وذلك دون تجاوز الخط الفاصل بين الحرب والسلام بنحو رسمي»

وما ذهب إليه «أنتونوفيتش» يكشف عن المكاسب التي تحققها حرب المعلومات لموسكو، فبينما تتحقق المصالح الروسية، لن يكون على روسيا الانخراط في صراعات مباشرة مع القوى الغربية، وكبديل عن ذلك يتم استعمال المعلومات في الصراع دون أن تتحمل موسكو تكاليف الحرب المباشرة، ناهيك عن افتقار الفضاء المعلوماتي لقوانين تضبط سياسات الدول ومواقفها إزاء بعضها بعضًا.

وبوجه عام تتمثل أهم الدوافع لمقاربة حرب المعلومات الروسية فيما يلي:[1]

1- خلق بيئة متسامحة Permissive environment : إذ إن حرب المعلومات تستهدف خلق بيئة متسامحة تجاه المصالح والرؤية الروسية، ولا يتوقف إيجاد مثل هذه البيئة على إدراج المعلومات التضليلية في

[1]- محمد بسيوني، نفس المرجع، ص 5.

سلسلة صنع السياسات على سبيل الحصر، ولكنه يمكن أن يجري عبر وسائل الإعلام الجماهيري والاجتماعية لإحداث تأثير في آراء وتوجهات الأفراد العاديين، ومن ثم جعلهم أكثر تقبلًا وتسامحًا مع الرواية الروسية الرسمية، وبالتالي تخفيف حدة المقاومة لسياسات موسكو. ولا يُمكن إغفال أن بزوغ قوى اليمين المتطرف في أكثر من دولة غربية يسهم في تدعيم هذا الهدف الروسي، لما لهذه القوى من علاقات تعاون مع موسكو.

2- تقويض القدرة على المواجهة: فالكثير من عمليات حرب المعلومات الروسية، وخاصة فيما يتعلق بالقرصنة الإلكترونية، تُضعف من إمكانات خصوم موسكو وقدرتهم على المواجهة، وهو ما تجلى بنحو كبير في الحرب الروسية الجورجية 2008، حيث إن الهجمات السيبرانية التي نُفذت في جورجيا بالتزامن مع دخول القوات الروسية أفضت إلى تعطيل استجابة جورجيا للغزو الروسي، لاسيما مع ما أدت إليه عمليات القرصنة الروسية من إضعاف قنوات التواصل بين الحكومة والجمهور، وإيقاف المعاملات المالية، بالإضافة إلى عرقلة انتقال المعلومات حول ما يحدث في مناطق الحرب إلى العالم الخارجي.

3- تشويه القوى المناهضة: ووفقًا لهذا الطرح وظّفت روسيا المعلومات لتشكيل سرديات وروايات تشوه القوى المناهضة لها، وفي الوقت ذاته تشييد صور إيجابية لحلفائها، فقد ظلت روسيا لسنوات تروج لمقولات أن الثورات الملونة التي شهدتها جورجيا وأوكرانيا كانت نتاجًا لمجموعات من المحرضين المدعومين من الولايات المتحدة كجزء من التدخل الخارجي المتعمد في كلا الدولتين من أجل إخراجهما من المدار الروسي. وقد استحضرت روسيا هذا النموذج أثناء الانتخابات التي شهدتها الدول الغربية في السنوات الأخيرة حينما وقفت بجانب تكتلات ومرشحين محسوبين على تيار اليمين المتطرف (على غرار مارين لوبان في فرنسا، أو حتى الرئيس الاميركي دونالد ترامب)، وتشويه صورة القوى المنافسة عبر توظيف الأدوات الدعائية والقرصنة الإلكترونية[1] .

4- إثارة المشكلات الداخلية: حيث تنطوي حرب المعلومات الروسية على التكريس لأوضاع داخلية مأزومة في المجتمعات الغربية، فحينما أثار الإعلام الروسي قضية الفتاة الألمانية (من أصل روسي) ليزا في عام 2016 التي ادّعت أنه تم الاعتداء عليها من قبل رجال لهم ملامح شرق أوسطية، كان يحاول الضغط على

[1]- محمد بسيوني، نفس المرجع، ص 6.

الحكومة الألمانية عبر استدعاء قضية اللاجئين بما تتضمنه من دلالات سلبية ضاغطة في الكثير من المجتمعات الغربية.

وعلى الرغم من تكشُّف اختلاق هذه الرواية من جانب الفتاة الألمانية، فقد كانت بمثابة تعبير عن توجه روسي للضغط على الغرب بملف اللاجئين، وليس أدل على ذلك من تصريحات وزير الخارجية الروسي «سيرجي لافروف» على خلفية القضية: «نتمنى لألمانيا وهي قاطرة الاتحاد الأوروبي كل النجاح في مواجهة المشكلات الهائلة مع المهاجرين، وألا تُخفي تلك المشكلات تحت السجادة، وألا تتكرر حادثة ابنتنا ليزا.« ومن جهةٍ أخرى، فإن عمليات القرصنة الإلكترونية تُحدِث خسائر فادحة في المجتمعات الغربية، خاصةً مع التوجه نحو مهاجمة البنية التحتية في هذه المجتمعات مثلما حدث في أوكرانيا في ديسمبر 2015 حينما تم اختراق شبكة الكهرباء في المنطقة الغربية إيفانو فرانكوفسك، وهو ما أدى إلى إيقاف عمل الشبكة وانقطاع الكهرباء في المنطقة.

5– مواجهة العقوبات الغربية: فعقب تدخل روسيا في أوكرانيا عام 2014، وضم شبه جزيرة القرم بعد استفتاء مارس 2014، تزايدت العزلة الأوروبية المفروضة على روسيا، واعتمدت الدول الأوروبية آلية للعقوبات ضد روسيا في مارس 2014 تتضمن عددًا من الإجراءات، كحظر التأشيرات، وتجميد الأصول، وفرض قيود تجارية واقتصادية. كما تزايدت العقوبات الاميركية المفروضة على روسيا. وفي هذا الصدد، مثَّلت حرب المعلومات أحد مسارات الاستجابة الروسية لهذه العزلة لما يمكن أن تلحقه من خسائر بالمجتمعات الغربية، ولذا فإن أحد التفسيرات التي طُرحت لعملية القرصنة التي تعرض لها الحزب الديمقراطي أثناء الانتخابات الرئاسية الأميركية عام 2016 كانت تصوير القرصنة على أنها ثأر من الحزب الذي وسَّع حزمة العقوبات الاقتصادية المفروضة على روسيا.[1]

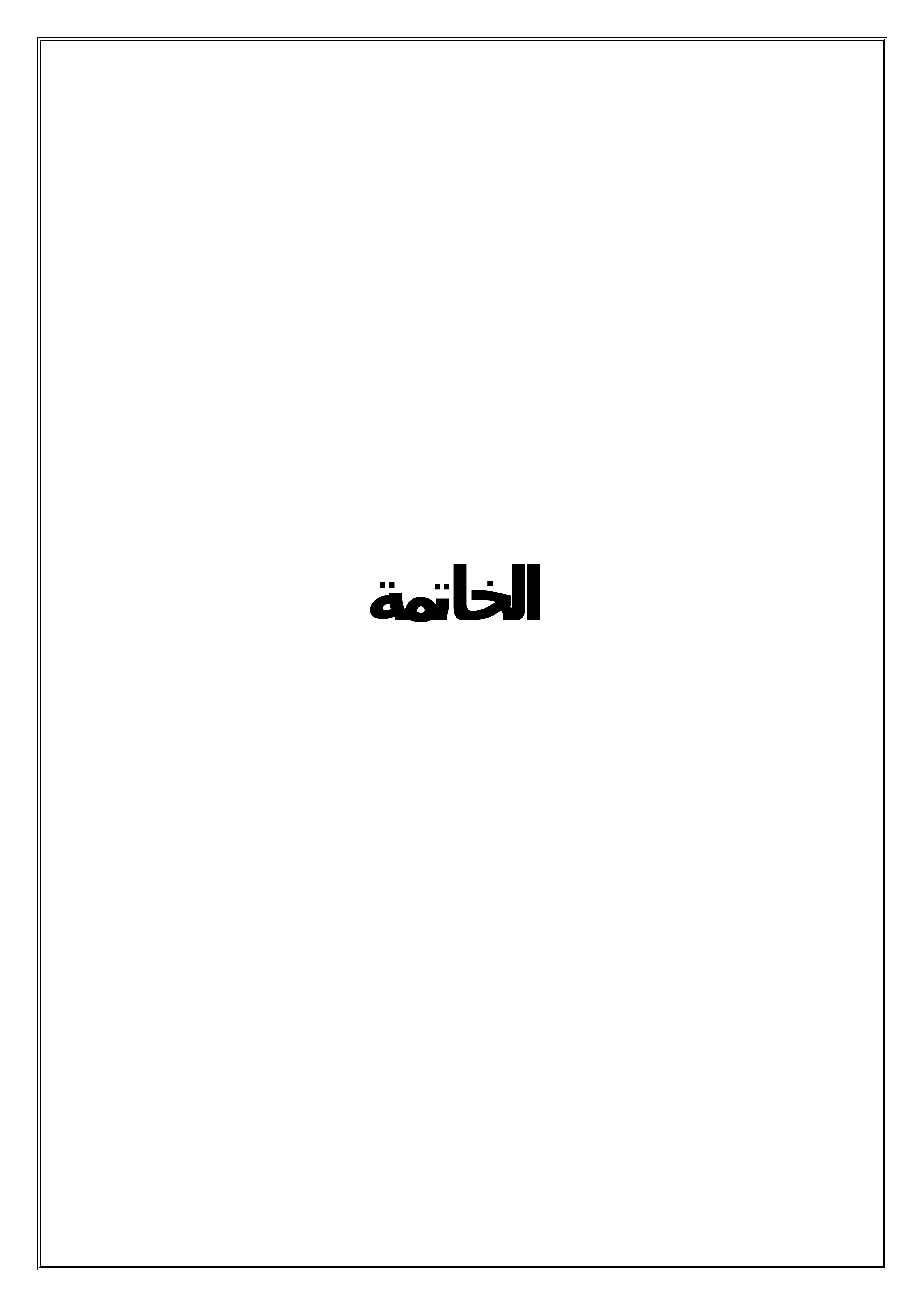
خلاصة القول.. ليس من المرجح أن تتراجع عمليات حرب المعلومات الدائرة بين روسيا والدول الغربية، فموسكو تصر على الحفاظ على نفوذها التقليدي وإرثها في الدول التي كانت ضمن المجال السوفيتي، وبالتالي فإن تقدم الغرب إلى هذه المناطق واستقطابه لهذه الدول سيدفع روسيا –بنحو أو بآخر– إلى التكريس لمدخل الحرب الهجينة Hybrid Warfare ، والتي تمتزج فيها الأدوات التقليدية وغير التقليدية، في تعاطيها مع

[1]– محمد بسيوني، نفس المرجع، ص 7.

الغرب، وخاصة مع تراجع إمكانية اللجوء إلى الخيار العسكري التقليدي في التعامل مع الولايات المتحدة والدول الأوروبية.

وتُعزز التحولات الراهنة في النظام الدولي هي الأخرى من تفعيل أدوات حرب المعلومات، فمع تعرض الولايات المتحدة لأزمات أثناء السنوات الماضية، والشكوك حول استمرارية قيادتها المنفردة للنظام الدولي، وبزوغ قوى منافسة (مثل روسيا) طامحة في المشاركة في قيادة هذا النظام، سيكون لحرب المعلومات جاذبيتها في إدارة العلاقات بين هذه القوى المتنافسة.[1]

[1]- محمد بسيوني، نفس المرجع، ص 8.



الخاتمة

من خلال ما سبق نستخلص ما يلي:

أن التعبير عن نهج الأمن السيبراني الناتج على شكل حماية متعددة المستويات فهو مركب متسع النطاق يبدأ بتطبيق نظام آمن للدولة ثم ممتلكاتها وجهتها وأفرادها البيع بعد ذلك كافة الدوائر التي يمكن أن تكون مصدرا للتهديدات.

وعلى تصاعد التحول الروسي لبناء إستراتيجية ناجحة للتصدي إلى مختلف التهديدات الإلكترونية سواء كانت في البيئة الداخلية أو الخارجية أو متداخلة بين الداخل والخارج وإنشاء حكومة إلكترونية، وتكشف الاعتماد على أدوات تكنولوجيا المعلومات والاتصالات.

أدركت الأجهزة الأمنية الروسية المختصة في كافة التهديدات الالكترونية والمخاطر السيبرانية أنه يتوجب عليها تأمين هذه المعلومات بشدة من خلال التحكم في الفضاء السيبراني.

حيث تختص روسيا في التعامل مع الكثير من التهديدات السيبرانية من خلال استراتيجياتها المنهية ما جعلها رائدة في المجال السيبراني.

لقد كان الهدف من الدراسة معرفة أهم التهديدات السيبرانية على التسيير الاستراتيجي للأجهزة الأصلية الروسية المختصة في تلك التهديدات.



قائمة المصادر والمراجع

قائمة المراجع:

الكتب:

1. حدّاد، **معجم مصطلحات الكمبيوتر والمعلوماتية إنجليزي – فرنسي – عربي**، (لبنان: مكتبة لبنان، د.ت).

2. سعد شاكر شابي، **الإستراتجية الأمريكية تجاه الشرق الأوسط**، (عمان، مكتبة الحامد للنشر والتوزيع، 2013).

3. **عادل عبد الصادق، الحروب السيبرانية : تصاعد القدرات والتحديات للأمن العالمي**، (المركز العربي لأبحاث الفضاء الإلكتروني، 2017/03/12).

4. عادل عبد الصادق، **الحروب السيبرانية؛ تصاعد القدرات والتحديات للأمن العالمي**، (إ.ع.م دبي: المركز العربي لأبحاث الفضاء الإلكتروني، 2017).

5. عادل عبد الصادق، **الفضاء الإلكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق**، (القاهرة: المكتبة الأكاديمية، 2016).

6. عبد الغفار رشاد القصي، **مناهج البحث في علم السياسة**، (القاهرة: مكتبة الأردن، 2005).

7. نوران شفيق، **أثر التهديدات الالكترونية على العلاقات الدولية، دراسة في أبعاد الأمن الالكتروني**، (القاهرة: المكتب العربي للمعارف، 2014).

8. نوران شفيق، **أثر التهديدات الإلكترونية على العلاقة الدولية**، (القاهرة: المكتب العربي للمعارف، 2016).

الدوريات والمجلات:

9. أحمد دياب، "**عودة بوتين: تحديات وطموحات روسيا بعد انتخابات الرئاسة**"، السياسة الدولية، العدد 188، المجلد، 47، (القاهرة: مركز الدراسات السياسية والإستراتيجية، أبريل 2012).

10. أحمد عبيس نعمة الفتلاوي، **الهجمات السيبرانية؛ مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر**، (العراق: مجلة المحقق الحلي للعلوم القانونية والسياسية، العدد الرابع، السنة الثامنة، 2016).

11. أحمد يوسفي الجميلي: **الشؤون العسكرية والأمنية**، (مركز صنع السياسات للدراسات الدولية والأمنية)، العدد الأول، 2018.البيت الأبيض، مكتب السكرتير الصحفي، "العلاقات بين الولايات المتحدة وروسيا: ورقة حقائق" إعادة تعيين "، بيان صحفي من البيت الأبيض، 24 يونيو/حزيران 2010.

12. بارة سمير، **الأمن السيبراني (cyber Security) في الجزائر السياسات والمؤسسات**، (الجزائر: المجلة الجزائرية للأمن الإنساني، عدد الرابع، جامعة قاصدي مرباح – ورقلة، 2017).

13. رغدة البهي، الردع السيبراني: المفهوم والإشكاليات والمتطلبات، (دبي: المركز العربي لأبحاث الفضاء الإلكتروني، 2017).

14. عادل عبد الصادق، **خطر الحروب السيبرانية" عبر الفضاء الإلكتروني**، (مصر: مجلة الأهرام لكمبيوتر الانترنت والاتصالات، مارس 2017).

15. عبد العزيز مهدي الراوي، "**توجهات السياسة الخارجية الروسية في مرحلة ما بعد الحرب الباردة**"، دراسات دولية، العدد 35.

16. فريدة طاجين، سياسات الدفاع الماليزية في ظل التهديدات الأمنية للبيئة الرقمية، واقع وتحديات، جامعة قاصدي مرباح، ورقلة، كلية الحقوق والعلوم السياسية.

17. فيصل يوسف، الأمن السيبراني والفضاء الإلكتروني، جريدة الموسم، السعودية، 2019.

18. قادير إسماعيل، **إدارة الحروب النفسية في الفضاء الالكتروني: الإستراتيجية الأمريكية الجديدة في الشرق الأوسط**، ندوة دولية بعنوان: عولمة الإعلام السياسي وتحديات الأمن القومي للدول النامية، (الجزائر: كلية العلوم السياسية والعلاقات الدولية، جامعة الجزائر 3، 2019/02/12).

19. كلثوم بيبيمون، **السياقات الثقافية الموجهة للهوية الرقمية في ضوء تحديات المجتمع الشبكي من التداول الافتراضي إلى الممارسات الواقعية**، (بيروت: مجلة "إضافات"، مركز دراسات الوحدة العربية، العدد 23، 2016).

20. لطفي لمين بلفرد، **الفضاء السيبراني: هندسة وفواعل**، (المجلة الجزائرية للدراسات السياسية، ENSSP، العدد الخامس، الجزائر، 2016.

21. منى الأشقر جبور، **الأمن السيبراني: التحديات ومستلزمات المواجهة**، (بيروت: الملتقى السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، 27-28 أغسطس 2012).

22. محمد بسيوني، **عقيدة جيراسيموف: دوافع الاستراتيجية الروسية لحرب المعلومات ضد الدول الغربية**، (المستقبل للأبحاث والدراسات المتقدمة، مجلة إلكترونية، 2017).

23. نبية الأصفهاني: **مستقبل التعاون الروسي– الإيراني في ضوء التقارب الأخير**، السياسة الدولية، العدد 144، المجلد 36، (القاهرة: مركز الدراسات السياسية والإستراتيجية، أبريل 2001).

المذكرات:

24. سمية طويل، **الإستراتيجية الأمنية الأمريكية في منظمة شمال شرق آسيا، دراسة لما بعد الحرب الباردة**، (أطروحة دكتوراه، كلية العلوم السياسية جامعة الحاج لخضر، تخصص علاقات دولية، 2009-2010).

25. إدريس عطية، الإرهاب في إفريقيا دراسة في الظاهرة وآليات مواجهتها، رسالة ماجستير، جامعة الجزائر.

المواقع الإلكترونية:

26. http://katehon.com/ar/article/hrb-lmlwmt-byn-rwsy-wlgrb-stnzf-wtwjyh-khty-llmwrd

27. http://katehon.com/ar/article/lmn-lsybrny-hd-lslh-lstrtyjy.

28. http://katehon.com/ar/article/m-ljdyd-fy-qyd-lmn-lsybrny-lrwsy

29. http://katehon.com/ar/article/m-ljdyd-fy-qyd-lmn-lsybrny-lrwsy

30. http://www.nytimes.com/2009/01/21/world/asia/21pstan.html

31. https://www.aljazeera.net/knowledgegate/books.

32. Senators Unveil Major Cybersecurity Bill Measure Would Update FISMA, Encourage Sharing of Cyber threats By Eric Chabrow, *February 14, 2012.* “Sen. Susan Collins, R-Maine, one of the bill's sponsors, said in a Senate speech. "The threat is not just to our national security, but also to our economic well-being." http://www.govinfosecurity.com/articles.php?art_id=4506&opg=1

33. Richard K. Betts.Conflict after the Cold War, Arguments on Causes of War and Peace, 2nd ed. (New York: Longman, 2002).

34. David Held et al.,Global Transformations: Politics, Economics, and Culture (California: Stanford University Press, 1999).

35. Joseph S. Nye.The Future of Power (New York: Public Affairs, 2011).

36. Electronic money regulations 2011 (EMR 2011) & the payment Services Regulations 2009.

37. The International Télécommunication Union, ITU Tool kit for Cybercrime Législation, Geneva, 2010.

38. Jarno Limnéll, Offensive Cyber Capabilities are Needed Because of Deterrence, *The Fog of Cyber Defence*, No. 200, 2013.

39. Catherine Lotrionte, A Better Defense: Examining the United States New Norms-Based Approach to Cyber Deterrence, Georgetown Journal of *International Affairs*, 2013.

40. Solomon, Jonathan, Cy**ber Deterrence between Nation-States: Plausible Strategy or a Pipe Dream?, *Strategic Studies Quarterly* 5**, No. 1, Spring 2011, Available at:

41. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA538310.

42. Stevens, Tim, **A Cyberwar of Ideas? Deterrence and Norms in Cyberspace**. *Contemporary Security Policy*, Vol. 33, No, 1, 2015.

43. Todd, Graham H., Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, *Air Force Law Review*, 64, No. 96, 2009.

44. Wilner, Alex S, Deterring the Undeterrable: Coercion, Denial, and Delegitimization in Counterterrorism, *Journal of Strategic Studies*, Vol. 34, No. 1, February 2011.

45. Putten, Frans-Paul Van Der, Minke Meijnders & Jan Rood, D**eterrence as a Security Concept against Nontraditional Threats, Clingendael Monitor**, 2015, pp. 1-64, Available at:https://www.clingendael.nl/sites/default/files/deterrence_as_a_security_concept_against_non_traditional_threats.pdf.

46. http://katehon.com/ar/article/hrb-lmlwmt-byn-rwsy-wlgrb-stnzf-wtwjyh-khty-llmwrd

47. Orji, Uchenna Jerome, **Deterring Cyberterrorism in the Global Information Society: A Case for the Collective Responsibility of States**, *Defence against Terrorism Review*, Vol. 6, No. 1, Spring & Fall 2104.



قائمة المحتويات

الفهرس

الفصل الثاني: الإستراتيجية الروسية للأمن والدفاع في فترة فلاديمير بوتين 2009-2014

الفصل الثالث: العقيدة الروسية في مواجهة التهديدات السيبرانية.